一部非虚构的美国情报界演义

国家窃听

专业剖析美国情报帝国黑白双面

真溱◎著



中信出版集团 CHINA CITIC PRESS

VISIT...

LANZAROTE Caliente.COM

一部非虚构的美国情报界演义

国家窃听

专业剖析美国情报帝国黑白双面

真溱◎著



中信出版集团 | CHINA CITIC PRESS

版权信息

书名:国家窃听

作者:真溱

ISBN:9787508645087

中信出版集团制作发行

版权所有•侵权必究

推荐序

帝国的B面

看完本书的头一回，我就意识到自己低估了这部书的价值和可读性。这不仅仅是一部引人入胜、一捧起来就让人欲罢不能，专事揭露当今世界唯一超级大国情报战、秘密战的著述。尽管单从文学意义上，作者文笔之漂亮，叙事之老到，绝不输于国内外任何一位纪实文学作家。但我想说，这不是本书的唯一长处。

一部出自职业情报人士之手的著作，却丝毫没有通常专业类书籍的枯燥和干涩，恰恰相反，作者倒更像是精于文学写作的老手，情节剪裁精当，细节铺排得体，故事跌宕起伏，不由让你感叹作者驾驭题材的功力。更让人不住点赞的是，专业性分析和见地随处可见，把美国情报业的风貌、架构、手段、流程，用文学笔法写来，让非专业者饶有兴味地读过之后，也能对什么是秘密战线，什么是情报战，有一种身临其境的印象和感受。更对我们今天的生活，在多大程度上被对手所窥伺和监控，产生出不寒而栗的忧思和警觉。

我至今还清晰地记得儿时萌生过的一个愿望，就是去做一名间谍。那时，来自北方大邻国的一本又一本间谍与反间谍小说，曾深深俘获过一个懵懂少年的心。这个永远不可能实现的梦想，几十年里，一直像一块被海浪击碎的船板，漂浮在暗夜的大海上，时起时伏，逐渐变成了一种纯粹的阅读兴趣。直到今天，我仍然对这类书籍保有浓厚的兴致，只要到手，就不会放过。

《国家窃听》再度点燃了我对儿时精神生活的某些记忆，所不同的是，它不是像当年那些虚构类作品一样，单纯靠波诡云谲、悬念不断的紧张情节吸引我，而是像个来自神秘国度的导游，用他手中挥动的小旗，一步步把我引进了世界上最神秘、最强大的情报帝国的大厦。

在这里，顺着作者的指点，你拾级而上，穿过重重沉重的铁门，又像剥洋葱一般，让你一层层去领略与你原先的想象十分不同的种种神

秘、阴谋、凶险和危机四伏，山重水复，柳暗花明，一个个似乎永远在隧道般的暗箱里运行的人物和事件，在最后一刻才豁然开朗，与我们在阳光下看到的一切大相径庭又相映成趣，读后让你顿生恍然大悟、原来如此的感叹。那些我们以为自己早就知道的事件的公开版，与不为人知的暗箱中的秘密，由于作者的巧妙对接，完成了对读者久困迷津的点化。

更为重要的是，《国家窃听》让我们又一次意识到，我们正在面对一个怎样的美国，一个自由女神的火炬之光照耀不到的“灯下黑”的美国。所有的帝国都有它的B面，正像所有光明鲜亮的招牌下，都有不可示人的黑暗勾当。这一点，从本书揭秘斯诺登事件及在全球引起轩然大波的章节中，得到了无可辩驳的诠释。读过这些段落，如果还有人一口咬定，这世上不存在阴谋，那他如果不是过于天真，就可能是制造阴谋者或者是其帮凶，舍此无他。

但如披露和洞悉阴谋，仅仅从情报揭秘的角度，似乎还不能穷尽真相或直达本质。小布什政府为什么执意要发动伊拉克战争？为什么对萨达姆必欲除之而后快？反恐，寻找大规模杀伤性武器，都是不值一哂的借口。甚至战后美国情报机构专门成立的调查委员会，公开承认这是一次“情报错误导致的战争”，仍不足以揭开这场战争带给世人的种种谜团。而当我们把这些谜团放在全球博弈的大背景下去观察，全部的谜底就会迎刃而解。

假如没有自1973年全球石油交易用美元结算，开始了真正的美元霸权时代，假如没有1999年欧元启动后，萨达姆执意宣布伊拉克的石油交易改用欧元结算，美国会不惜甩开联合国也要打响伊拉克战争，并在攻陷巴格达后马上着手成立伊拉克临时政府，而临时政府成立后宣布的第一条法令，就是伊拉克的石油交易，从欧元结算改回用美元结算——还有比这更令人信服的谜底和答案吗？可悲的萨达姆恐怕至死也没弄明白这一点，他不知道自己的一次自作聪明之举，踩到了美国霸权的底线——不可动摇的美元地位，最终把自己送上了绞刑架。这是比美国情报界的一切秘密都更重大的美国国家机密，所以，美国才会在战后，宁肯承认“一开始就错了”，是由于“情报失误”，但也决不会承认这一更高的国家机密存在的原因。

不过，这已超出了情报工作者分析情报的范围，而已进入到国家大战略分析的层面，我无意对《国家窃听》的作者进行苛求。因为仅就本

书而言，它已出色地完成了它所能承担的任务，使每个读到它的读者，从中了解为什么这个世界会不断发生、正在发生、将要发生那么多令人不解的诡异事件，那么多的“颜色革命”及动荡暴乱，因为这一切，都与一个国家以及它的国家利益紧密相联；因为这个国家正在与整个世界玩一场零和游戏：你的失去，就是他的获得，赢家通吃。这就是帝国最高最深的秘密。而这个秘密，正是一切帝国，包括美国永不示人的B面。

谨以以上观感，为《国家窃听》作序。

乔良

国防大学教授

空军少将

2015年7月17日于乌鲁木齐

既看热闹也看门道

拿到真溱研究员这本《国家窃听》的时候，距斯诺登揭开“棱镜”计划已经过去将近两年。我拿着打印稿，几乎一口气看完，受益匪浅。这是一部独特的作品：以专业严谨的学者风格写出了生动精彩的故事。无论你是看门道，还是看热闹，本书都不会让你失望。

首先，本书大量的细节和资料基于系统、审慎、细致的专业研究。目前，全球关于斯诺登事件的图书已经有好多本，但作者基本还是以记者为主，专家级的著作还没有。《国家窃听》可以满足你对于斯诺登揭秘的美国情报监控系统的所有好奇。

其次，本书在专业的基础上，突出了可读性。整本著作最难的不是把专业性更好地体现出来，而是在专业信息基础上，写成扣人心弦的故事。本书大量的情节、人物和场景，不是出于简单的虚构和想象，而是基于海量的资料。穿针引线，融会贯通，旁征博引，梳理了从“二战”到冷战，再到今天网络时代的美国情报体系，梳理了历史的重大事件，将其有机地关联起来。

当然，本书最让我受益的还是其丰富的知识性。大量的细节描述源

自作者在资料收集上的无与伦比。它甚至比目前很多研究“棱镜门”的专业论文涉及的知识面更加广博，书后的648项参考文献就是最好的证明。

人们对于“棱镜门”的关注更多从新闻事件的角度出发，那么，事件发生两年之后，再阅读这样一本书，究竟还有多大的价值。要理解这一点，我们必须重新认识“棱镜门”。

可以说，“棱镜门”事件是互联网界经历过的最重要的事件。无论是其全球性的新闻效应，还是从中逐渐释放的社会启蒙意义，以及它对于全球网络空间规则与秩序的影响，都超越了迄今所有的与互联网相关的事件。对于人类正在进入的网络空间主导的新时代，“棱镜门”的深层次价值和影响才刚刚开始展现。网络空间的秩序和边界，网络空间的国际地缘政治格局，也是在“棱镜门”之后才逐渐显露出问题。

所以，两年时间正好。没有短到我们来不及从容进行深入思考，也没有远到让人们淡忘和漠视。就像直到今天，斯诺登继续披露的信息依然会引发全球媒体重要版面的高度关注。关于斯诺登事件的思考更远远没有结束，甚至依然还只是开始。

“棱镜门”：互联网的成人礼

斯诺登事件究竟重要到什么程度？如果把互联网比作一个人，那么斯诺登事件就是一个人的成人礼。互联网诞生在美国，美国的体制和技术创新孕育了互联网。但是，当互联网经历了这次成人礼，则标志着美国与互联网之间出现了责任与权利的分水岭。

在斯诺登的各种称号中，大概再也找不到比“21世纪的切·格瓦拉”更恰当也更富有内涵的称号了。“斯诺登是新的切·格瓦拉吗？”美国《外交政策》刊文说，他没有共产主义革命者切·格瓦拉的样貌，但这不能阻止斯诺登成为这个时代的一个全新符号。网络空间已被视为继陆、海、空、天之后的“第五空间”。第五空间不但超越了现实空间，而且开始影响并主导现实空间。所以，21世纪的革命主战场就在网络空间。切·格瓦拉作为20世纪最富传奇英雄色彩的历史人物已经留在历史中，而在以21世纪为分水岭的新的网络时代，无疑也在呼唤这样一个符号性人物。

美国除了担当现实空间的世界警察之外，也成为网络空间的世界警察。美国安全局“搜集一切”的全球监控计划，就是为这个战略目的服务。如果说，19世纪独霸全球的力量在于制海权，20世纪的力量在于制空权，那么21世纪的力量就在于制网权。建立这样一套全球、全网和全息的独一无二的监控体系，对于完成像奥巴马所说的“美国还要再领导全球100年”的霸权梦想，无疑是最重要的基础。

挑战这个以牺牲全球所有国家和民众基本权益和基本安全的疯狂系统，成为斯诺登们的最高使命。斯诺登改变的将不仅仅是美国监控的进程，也不仅仅是全球互联网治理的进程，而是整个人类文明的进程。当然，历史也将从此彻底改变他的人生！

所以说，“棱镜”计划是非同寻常的宝藏。我们对于“棱镜”计划的掌握，还只是冰山一角。对于“棱镜”计划的深度研究，还远远不够。关于它对现在和未来的影响，更是缺乏战略性的预估。

两年过去了，被历史改变的斯诺登，至今依然困顿于俄罗斯，美国政府的监视行为依然故我，全球的互联网规则的未来之变依然混沌不清。这也意味着，斯诺登与我们这个时代的故事，远远没有到收尾的时候。因为目前长篇累牍的新闻报道依然局限于新闻事件本身，而对于事件背后信息的挖掘，尤其是对于政府监控公民私人信息的分析，对于本次事件真正的主角——美国国家安全局的揭露，以及对于网络时代公民隐私和政府权力的边界的探讨，还远远不够。

中国社会启蒙与战略觉醒

“棱镜门”与中国的相关性与意义，可能远远超过人们的想象。可以说，正是斯诺登事件掀起了中国网络空间最大的一次社会启蒙，也促动了一次战略觉醒。

历史总是如此戏剧化：斯诺登选择香港为出逃的登陆点，以欧洲媒体为内幕第一披露渠道，最终以俄罗斯为落脚点。一下子玩转了美国、中国和整个欧洲等现实世界最核心的全局性地缘政治版图。当然，这个事件对于中国的影响和意义尤其重大，因此，2013年可以称为中国网络空间战略觉醒之年，并直接推动2014年成为中国网络空间战略的奠基之

年。围绕国家网络空间战略的顶层设计不断快速进入议程，而且相关部门加速推进和落实战略，这将全面、深刻地影响和改变未来中国互联网的发展。

“棱镜门”最大的作用就是生动呈现了网络空间模糊的边界和混乱的规则，尤其是美国滥用霸权的真切现实。斯诺登披露的文件中，大量被标记为“绝密”，在那些制作粗糙的幻灯片中，美国国安局反复吹嘘自己进行监控的工作目标就是：“无所不及”“无所不晓”“无所不用”“无所不采”。从NSA（美国国家安全局）的绝密幻灯片演示文稿中，仅标识为“NSA战略伙伴”的跨国企业就有80多家，远远超过了“八大金刚”。IBM（国际商用机械公司）、思科（Cisco）、微软、雅虎、谷歌美国在线、Skype、YouTube、惠普、苹果等几乎美国所有重要的高科技公司都卷入其中，成为美国情报机构“一网打尽”监听项目的重要基石。美国高科技企业事实上已经成为美国政府掌控和监控全球互联网的重要一环。

斯诺登事件给我们带来的另一大启示是，美国人利用互联网为国家安全、反恐、维护国家利益等方面做了很多具体的工作，并在反恐等领域取得效果。根据美国国家安全局前局长基思·亚历山大的说法，“棱镜”计划曾帮助政府成功挫败了约50次恐怖袭击阴谋。其中的确有一些方式方法值得我们学习。首先，开发利用社交媒体的公开数据促进维护公共秩序，使用专业分析工具后，社交媒体上的输出会有新的含义，有助于识别恐怖分子；其次，对海底光纤通信数据、出口数据进行有效监测、存储和分析，辨析有价值信息，在全球范围内锁定具有恐怖主义倾向的可疑分子；第三，善于利用诸如Palantir等公司提供的海量数据分析平台，借助前沿IT技术与企业为美国反恐大数据分析、识别等任务提供良好支撑。

对照美国在互联网管理和利用方面的做法，可以映照出中国各层面的不足。在认清现存的一些不足的基础上，要善于学习美国打击网络犯罪、进行网络治理创新的方法，尤其是在反恐等方面的先进理念与手段，创新安保方式方法，建立自己过硬的攻防力量，准确打击破坏网络安全和国家安全的组织与个人，为全球互联网发展贡献中国力量和中国价值。

方兴东

互联网实验室创始人

数字论坛发起成员

中国信息化百人会成员

浙江传媒学院互联网与社会研究中心主任

自序

2013年6月的某一天，人们突然发现，一个面色苍白、瘦削、戴着眼镜、留着一点儿髭须的年轻人成为新闻人物。大家还知道他的名字叫爱德华·斯诺登。和这个名字一同出现的，还有一个并不常用的词语，叫作“棱镜”。经过他的爆料，人们才知道，这个“棱镜”原来是美国的一项高度机密的情报计划，硅谷里最有名的几家公司，不管是否声称自己“不作恶”，事实上都参与其中。

也就是从那一天起，几乎每天都会有关于美国小伙儿斯诺登的新闻。他就像哆啦A梦，肚子上有个神奇的百宝袋，总有猛料爆出，而且不经意就能登上头版头条。到年底，积累了很多人气的他，毫无悬念地被多家媒体评为当年的新闻人物。

不过，由于他爆出的料实在太多，那些材料在经过记者的筛选和转述之后，更显得支离破碎。对大多数人而言，此事的头绪越来越厘不清，甚至产生了一种“阅读疲劳”——人们只要看到文章标题上有“斯诺登”三个字就跳过去，不再细读。随后，有一些好心人把已掌握的资料稍加整理、汇集成册、印刷出版，可惜他们过于匆忙，来不及追本溯源，更做不到正本清源，混乱的情况越发严重。

“棱镜”计划到底是怎么回事？为什么斯诺登只是一个契约合同雇员，却可以掌握如此之多的秘密？他为什么要曝光这些秘密？

这是一些非常基本的问题，挥之不去也不能回避，想要回答清楚也并非易事。美国有着当今世界最为庞大且复杂的情报圈，他们自诩的“情报界”，是当之无愧的情报帝国。“二战”之后，他们逐步形成了一整套情报搜集、情报分析的策略、方法、手段和系统。对于情报搜集工作，美国人还使用另一个术语，叫作“情报监视”。“情报”也好，“情报搜集”、“情报监视”也罢，原本就是美国情报界非常敏感的话题，公开的资料有限。寻找有关“棱镜”计划的这些基本问题答案的过程，也就成为揭开美国情报帝国秘密的一次难得经历。

对“斯诺登现象”以及他揭露出来的资料进行解读，当然是最为直接的揭秘线索。其他一些重要线索原本散落在陈年的报刊文章之中，隐藏

在众多的访谈演讲和证词里面，长期被人忽略，现在它们则被拂去尘土、重现光彩，被赋予了新的意义。

对美国这个情报帝国而言，最近一次重大的历史事件就是“9·11”恐怖袭击事件。这也是本书故事叙述的起点。这一事件深刻改变了冷战结束后美国人对情报以及情报搜集的看法。1978年美国政府颁布的《外国情报监视法案》对美国情报界进行了严格的约束，美国政府发现自己的情报工作被这部冷战期间的法案严重限制了，到了不改不行的地步。这一诉求在《美国爱国者法案》中得到初步解决。在随后进行的“反恐战争”当中，情报还被用作发动战争的借口，这一“用途”自然被人唾弃，但毫无疑问的是，在“擒贼先擒王”的过程中，情报以及情报分析无可争议地成为制胜的利器。

就在“9·11”恐怖袭击事件之后不久，美国政府启动了极为秘密的情报监视计划。尽管有了《美国爱国者法案》，这一计划的部分内容在法律上仍然存在争议，美国政府高层不得不严格控制知情范围，以此避免法律方面的麻烦。即便如此，几年后，《纽约时报》还是得到了一些线索并将其公之于众。作为回应，美国国会不得不在《美国爱国者法案》之后，再次对《外国情报监视法案》进行修订，先是颁布带有临时约法性质的《保护美国法案》，然后是2008年的《外国情报监视法案》修正案。就在这部修正案颁布前的几个月，另外一项极为秘密的情报监视计划付诸实施，这就是“棱镜”计划。

美国政府在情报搜集的技术和数据方面一向广泛借助商业公司的力量，这并不是什么新鲜事，至少在“二战”期间就已经如此，冷战期间亦是如此，现在更是如此。“棱镜”计划之所以夺人眼球，是因为参与其中的各个公司极负盛名、拥趸无数。随着笼罩在“棱镜”计划上的神秘面纱一层一层被揭开，可以清楚地看到它其实只是美国那庞大情报帝国的冰山一角。

冷战结束后的十多年间，美国人一直认为自己没有什么对手，情报帝国的力量相应地被大幅度削弱，直到“9·11”恐怖袭击事件，他们发现自己的情报搜集、处理和分析力量严重不足，短期内还不可能建立起一支属于政府的庞大队伍，只能广泛依靠社会力量。这就滋养了一批可以在政府和公司之间自由“旋转”的精英，也养肥了一批能够有门路拿到高额合同的“旋转门”公司，其中一个公司名叫“博思–艾伦–汉密尔顿”。这便是斯诺登最后工作的那家公司。但实际上，他们承担的项目来自一个

非常神秘的政府部门：美国国家安全局。

书归正传。

时光机已经转动，我们现在就回到十多年前那改变世界的一天。

楔子

几乎所有人都记得，那一天非常晴朗，空气非常透亮。

佛罗里达州萨拉索塔。

安德鲁·卡德（Andrew Card）很早就醒了。作为白宫幕僚长，他已经习惯每天早起。[1]差不多一周之前，小布什总统刚刚结束了一个漫长的假期，也追平了多年以前尼克松总统创下的休假纪录：整整30天时间，他都在得克萨斯州的大牧场里度过，非常潇洒惬意。当然，他每天还是要花一些时间听听汇报、做做工作。[2]前一天晚上，小布什（George W.Bush）宴请了他的弟弟、佛罗里达州的时任州长杰布·布什（John “Jeb” Bush），以及前任州长等一班人，宾主相聊甚欢，气氛轻松愉悦。[3]

卡德现在记挂的是另外一件事情：总统约好了要和记者一起晨跑，比试一下，可此时正赶上海边出现红潮，海滩上有海水冲上来的大批死鱼，发出阵阵恶臭。这样的气味，多半儿会让小布什不舒服。一直等到总统兴高采烈地回来，卡德那颗悬着的心才算放了下来，显然记者跑输了，小布什轻松取胜。看起来，这是一个好兆头。这一天也将是很轻松的，幕僚们只给总统安排了一项“软性活动”，他将走访当地一所小学，为二年级的学生朗读课文，也算是为他主持签署的“有教无类”法案造一造声势。[1]总统的专车在8点半准时离开驻地前往学校。[3]

华盛顿特区。

总统在外地休假，中央情报总监乔治·特内特（George Tenet）便可以忙里偷闲，不用准备《总统每日简报》，也不用起早贪黑参加每天例行的情报通气会——那样的话，他需要在大概清晨6点半之前就离开家去白宫。[4]就在总统登车即将前往小学的那一刻，特内特正在距离白宫三个街区的圣瑞吉斯酒店，和亦师亦友的前参议员戴维·博伦（David Boren）共进早餐。他们的座位临街，透过窗户可以看到外面亮丽的风景。[3]遥想当年，博伦是参议院情报特别委员会主席，特内特还只是个毛头小子，多亏博伦慧眼识珠，一手把特内特提拔为参议院情报特别委员会办公室主任。[5]正因如此，特内特对博伦一直心存感激。

在整整一个夏天中，情报总监越来越担心一件事情：美国可能正在面临一次严重的恐怖袭击。情报部门里到处可以听到这样的声音：要出大事了。反复出现的预警报告让他夜不能寐，朋友们都认为这段时间，情报总监总是一副心神不宁的模样。[3]他对国家安全委员会里负责反恐问题的理查德·克拉克（Richard Clarke）说："我的第六感告诉我，有事情要发生，而且是大事情。"[6]

来自方方面面的情报所反馈的信息一致，显示出恐怖袭击即将发生，但是特内特手里还缺少最为关键的情报：恐怖袭击将在何时、何地发生。他没有办法打消国防部部长的疑虑，这会不会只是一场大骗局。更不妙的是，特内特与国家安全事务助理康多莉扎·赖斯（Condoleezza Rice）素有芥蒂，除了每周例会之外本来就联系不多。但听完中央情报局反恐中心的报告后，特内特实在坐不住了，他决定马上去见赖斯。这样做，除了可以把事情当面汇报清楚外，他更希望通过这种例会之外的见面，让赖斯有所震动，深切感受到当前威胁的严重性，从而敦促总统立刻采取行动。在他看来，反恐中心的报告听起来让人毛骨悚然，"在未来几周或者几个月内美国将遭遇一次严重的恐怖袭击"、"在过去24小时中搜集到的7份情报都说明袭击迫在眉睫"。可是情报总监等来的只是赖斯彬彬有礼的接见，仅此而已。7月的这次会面让他失望透顶。针对恐怖袭击的反制计划被列上了议事日程，一切都四平八稳、按部就班，但形势已经火烧眉毛，如此准备相当于没有准备。[6, 7]的确，赖斯后来回忆，自己当时全部的心思都放在了导弹防御方面，便将恐怖威胁这件事放心地交给了国家安全委员会。[8]

只是自己着急也没用，于是，特内特干脆放下工作，外出休假了一段时间[9]。8月下旬，特内特又接到一份报告，说是抓住了一名嫌疑犯，此人想到明尼苏达州的飞行学校去学习开飞机。联邦调查局要求中央情报局和国家安全局（下文分别简称"中情局"和"国安局"）对他的电话进行监听，很快就搜集到了一大堆有关他的材料。[3]特内特专门飞到得克萨斯，见到了正在休假的小布什。总统兴致勃勃地开着自己的皮卡，带着特内特在草原上兜了一大圈儿。原本想去汇报工作的特内特没敢破坏小布什的心情，两个人聊的只是花草树木、鸟兽虫鱼之类的轻松话题。[10]有关恐怖袭击正在靠近的种种情报，包括那个想学飞行的嫌犯的情报，他最终都没敢向总统汇报。[9]

马里兰州米德堡。

这是退役军官托马斯·德雷克（Thomas Drake）到国安局上班的第一天。清晨5点，天还没亮，他就按照要求急急忙忙赶到了上司的办公室。[11]局里资深的技术专家威廉·宾尼（William Binney）则请了一天假，一早就带着岳父去看眼科医生了。各种检查要花很长时间，宾尼现在能做的就是坐在休息室里等待。[12]

国安局局长迈克尔·海顿（Michael Hayden）前一天晚上熬夜看完“星期一足球夜场”才睡觉，但这并没有影响他按照正常时间起床洗漱。早上7点，他还理了理头发。上班途中，海顿经过了一栋三层小楼，那里是“国家安全行动中心”，也是他的战时指挥部。海顿走进自己的办公室时，下属已经准备好向局长简要报告各方面的最新情况，接下来，海顿还要在8点15分和新任命的“平等就业委员会”主任碰一下头。[13, 14]

距离海顿局长办公室所在的国安局总部不远，有一家小小的动漫公司，那只是几个嘴上没毛儿的孩子创办的。他们雇用的也都是些毛孩子。其中有一个男生，之前生了好几个月的病，后来索性不再去学校了。虽说还只是个高中生，他已经把计算机玩得很溜了，看得出来他很喜欢鼓捣这些东西。公司不大，考勤做得倒是有板有眼。尽管时间还早，这个男生已经在开车上班的路上了。[15]他的名字是爱德华·斯诺登（Edward Snowden）。

看起来，正常运转、安稳寻常的新一天又开始了。

但是，几个小时之后，所有的一切都脱离了原来的轨道。

这一天是2001年9月11日，星期二。

第一回 以反恐的名义

白宫。

2001年9月11日深夜。在忙碌了非同寻常的一个整天之后，小布什总统终于安顿了下来。保卫部门建议他在紧急行动中心地下战情室外面的一个小房间里过夜。他很清楚，那里只有一个破沙发和一张折叠床。在这样的地方，他是根本睡不着的，因此他坚持回自己的卧室去。可上了床，他才发现想要入睡并不容易，白天发生的事情一幕一幕不停地浮现在眼前：一架飞机撞向大楼，又一架飞机撞向大楼，双子塔倒塌，五角大楼冒起黑烟……他好不容易在蒙眬中感到要睡着了，却猛然间听到有人在喊："总统先生，总统先生，白宫受到攻击了！我们快走！"[16]

这非同小可！

小布什立刻就醒了。他赶紧叫醒夫人，夫人没有时间去戴隐形眼镜，看不清路，只能让他牵着。总统自己顾不上穿鞋，光着脚，只穿着T恤和运动短裤，一手拽着夫人的睡袍，一手牵着爱犬，嘴上还招呼着另一只爱犬，跟着特工匆匆忙忙地逃进了地下防空洞。他们穿过一道又一道大门，终于到达安全的地方：紧急行动中心。这是冷战初期为了应对重大袭击修建的一座坚固的地下堡垒，24小时有军事人员守卫，并且配备了充足的食物、水和电力供给，可以保障美国总统一家人很长一段时间的生活[16]。

几分钟后，一个军官走进战情室，表情严肃地向惊魂未定的小布什报告："总统先生，那是咱们自己的一架飞机。"[16]

这一天对小布什的刺激让他刻骨铭心。他对自己的幕僚长卡德说："你现在看到的是21世纪的第一场战争。"[16]在他心里已经有了一个明确的决定：必须反击。和他的父亲一样，小布什每天都会写日记。那天夜里，他写下了这样几句话："恐怖暴徒想让我们成为他们的人质，我们绝不答应。我希望这将为我们提供一个机会，联合全世界的力量反对恐怖主义。""21世纪的珍珠港事件就发生在今天。"[3]

立法先行

美国自诩为法治国家。小布什心里十分清楚，要发动一场以反恐为主要诉求的战争需要什么：

让国家进入战争状态不仅仅需要加强国防设施建设，还需要更强有力的法律、财政和情报工具，以便及时发现并阻止恐怖分子的行径，否则就太晚了。[17]

“9·11”事件发生之后，美国司法部部长约翰·阿什克罗夫特（John Ashcroft）很快就召开了一次记者招待会，敦促国会在一周之内通过司法部的立法计划。他这一招很管用。在当时的情形之下，国会方面如果稍有怠慢，必然会招致严厉抨击，比如“在恐怖主义面前，表现软弱”。国会只能尽快完成立法过程。9月19日，国会和司法部各自拿出一份草案，坐下来交换意见。两份草案在许多重要方面非常相似，但司法部的提案更加激进，因而争论不可避免。司法部部长态度强硬，他说，立法过程如此缓慢，让人非常担心，“争论不能阻止恐怖主义”。[18]国会方面只得快马加鞭。

2001年10月26日，《美国爱国者法案》获得通过。这一天距恐怖袭击发生仅仅45天。争议被暂时搁置，带有争议的条款被打上“日落”标签，也就是说，这些条款只是暂时有效，等到“日落”的时刻一到，就要重新拿出来审议。又经过一番讨价还价后，新法案的“日落”时间被敲定在2005年。[18]

所谓“爱国者”，并非来自《美国爱国者法案》的正式名称。的确曾有个别人望文生义，把这项法案看作美国人惩治内奸的法律，闹出了笑话。[19]法案有一个可简单释义的题目，翻译成中文就是“以适当手段监听并阻止恐怖主义，使美国更团结更强大之法案”。美国人也很喜欢玩文字游戏，这句话的几个英文单词首字母缩写正好是“PATRIOT”，也就是“爱国者”的意思。顺便说一句，这个法案还有一个更长的副标题，翻译成中文就要稍微费点儿劲儿了，意思是“旨在阻止和惩罚发生在美国和世界各地的恐怖主义行为，加强执法调查手段等的法案”。

小布什后来在回忆录里说：他本人对于这部法案有一个遗憾，就是

它的名称。白宫将法案提交给国会的时候，它的名称原本是“2001年反恐法案”，是国会自作聪明，改成了现在这个题目。这样做，的确别有意味，那些反对这项法案的人很容易被不明就里的普通民众认为是不爱国的。这样一来，多多少少给那些对法案提出异议的议员们造成了无形的政治压力。小布什说，这并非他的本意，并且表示自己“本应在签署法案之前敦促国会把名字改掉”[17]。这多半只是一种事后遁词，因为他并没有那么做。

从本质上讲，《美国爱国者法案》是一部情报法案。它的重要内容之一是对1978年颁布的《外国情报监视法案》做出重大调整，放宽了对情报部门开展监视活动的限制，为美国安全和情报部门以反恐为由监听普通民众的电话和互联网通信打开了方便之门。比如法案第二章中的“增强的监视程序”那一条目的主要内容是这样的：

（1）把恐怖主义和计算机犯罪纳入监视范围（第201、202条），扩大了情报监视的适用范围。

（2）有关部门可以在未经司法审查的情况下获得与美国公民有关的敏感信息（第203条）。

（3）有关部门可以对拥有多部电话的个人进行机动式监听，也就是说，有关人员可以根据需要，同时对这个人的家庭电话、单位电话和移动电话等多部电话进行监听，而在此之前，监听个人的不同电话需要分别申请许可（第206条）。

（4）监听期限可以延长到90天。如果涉及外国人或国外机构，监听期限可以延长到120天甚至一年（第207条）。

（5）语音电子邮件也被纳入电子情报监视范围（第209条）。

（6）有关部门可以在未经司法审查的情况下，要求通信商提供客户的详细信息，包括姓名、地址、本地及长途电话记录、身份记录、服务的时间和类型、付款方式、银行账号和信用卡号码等（第210、211条）。

（7）有关部门可以在不告知当事人的情况下，搜查他的办公地点或者住所，事后再出示法院许可（第213条）。

（8）有关部门可以获取民众的教育、医疗、投资、信用等各种记录（第215条）；等等。[20, 21]

这其中的最后一项内容，也就是第215条引起了很大争议。尽管法律条文上并没有出现“图书馆”或者“书店”的字样，但在2001～2002年，来自图书馆界的反应最为激烈，以至于许多人把这一条称作“图书馆之规”。网络杂志《沙龙》上登出了一篇文章，题目很有点儿“标题党”的意味——“他知道你借了什么书”，还配上一幅插图，正襟危坐的山姆大叔紧紧盯着惊呆了的读者。《旧金山纪事报》的文章题目更加惊人：“联邦调查局调查美国人的阅读习惯”。其他一些媒体也刊登了类似的报道。[22]

说起来，联邦调查局（FBI，简称“联调局”）和图书馆界在历史上曾经闹过不愉快。1987年，纽约市的一个图书馆员向美国图书馆协会（ALA）反映，联调局要求他们提供来自“敌对国家”的那些人的阅读情况。紧接着，全美各地的图书馆陆续打电话给协会，说是接到了类似的通知。联调局已悄悄进行了几十年的“图书馆感知”计划就此曝光，但也就此中止。[23]

图书馆界斗争了几十年，终于使华盛顿特区和48个州制定法规：未经法律授权，图书馆员不得发布读者借阅图书的信息。市面上出售的图书馆借阅管理软件绝大部分会在读者还书之后自动抹去他的姓名信息，为的就是保护读者隐私。[23]《美国爱国者法案》如果通过，就意味着图书馆界经过多年奋斗得到的成果一夜之间灰飞烟灭。作为美国图书馆界最大的组织，图书馆协会不能坐视不管，可惜他们的各种行动于事无补。这部法案毫无悬念地得到了通过，在众议院和参议院的投票结果分别是357：66和98：1。

参议院表决时的唯一一张反对票是由参议员罗素·菲因高德（Russell Feingold）投下的。在当时的社会大环境中，要做到这一点，需要拥有特别强健的心脏。在投票前，菲因高德还发表了长篇演讲。他说：

让我最为不安的一项规定是，允许政府利用《外国情报监视法案》强制各个行业提供每个人的信息记录，条件是这些信息可以被用于调查恐怖主义或者间谍活动……新的规定要求所有业务活动记录都可以被强制提供，包括那些含有个人敏感信息的记录，例如由医院或者医生提供的医疗记录、受教育记录，甚至某个人从图书馆借阅图书的记录。这项

法案极大地扩张了政府权力，却只提供了非常少的司法监督操作方案。[24]

菲因高德反对的不仅仅是这个法案里的第215条，他反对的是当时被很多人接受的以自由换取安全的想法。即便知道自己是孤军奋战，菲因高德仍然毫不畏惧地发出了自己的声音：

如果我们生活在一个警察国家，抓住恐怖分子可能会容易一些……但是扪心自问，我们无法要求我们的年轻人为这样一个国家去战斗、去牺牲。简而言之，这不是美国。我们是为了捍卫自由才投入这场新的反恐战争。但如果我们牺牲的是美国人民的自由，那么战争还没有打响，我们就已经输了。[24]

事后来看，激起图书馆界热议的第215条又多少像是在玩“障眼法”，目的是让人们真正该担心的事情得以悄悄过关。绝大多数人想不到，这个貌似简单的条款背后蕴含着巨大的潜力和能量，甚至超出了把它写进《美国爱国者法案》的那些人的想象。每隔几年，这个第215条都会被再次提及，成为经久不息的争议焦点。

在这部《美国爱国者法案》里，最常见的句式是：本法案对《美国法典》（USC）或者《外国情报监视法案》等法律的某章、某条、某款进行修订，修订的方法是删除原来法律文件中的一些标点、单词和语句，然后插入一些标点、单词和语句。

所以，阅读法案原文是一件极为痛苦且乏味的事情。可别忘了，《美国爱国者法案》不是仅有几页纸的小文件，而是一份有上百页的大文件。读着读着就会产生一种错觉，感觉自己在看一个被修订的Word文档，并且会把每一处修订都念出来。这或许叫作严密严谨，但有点儿让人不知所措。随便找一条来看看吧。比如第202条，是这样写的：

对《美国法典》第18卷第2516章第1条第c款进行修订，删除“和第1341章（与邮件欺诈有关）”，插入“第1341章（与邮件欺诈有关），违反第1030章（与计算机欺诈和滥用有关）”。[20]

想知道这一条规定了什么内容，需要把《美国法典》的第2516章第1条第c款找出来，在完成删除和插入操作之后，才能知道。

在美国，新的联邦法律总是以单行法的形式发布，到年底编入编年

体的《美国法律总汇》和主题归纳式的《美国法典》之中。所以，《美国法典》并不是一部法律，而是美国联邦法律的总汇。共有多少部法案被《美国爱国者法案》修订过呢？据统计，超过了15部。[23]除了上面提到的《外国情报监视法案》，还有《电子通信隐私法案》（ECPA）、《洗钱控制法案》（MLCA）和《银行保密法案》（BSA）等。

总而言之，《美国爱国者法案》降低了执法部门获取搜查令和扣押令的门槛，增加了执法的随意性。所以，从这个法案颁布之日起，就不断有人认为它违反了美国宪法，这中间既有专家学者、民间人士，也有国会议员、联邦法官，民间组织，甚至一些地区的法庭和政府也发出了不同的声音。2003年4月，89个城市通过了谴责《美国爱国者法案》的决定。到2004年10月，350个市镇的5400万美国公民投票指称《美国爱国者法案》中部分条款对民众自由造成了威胁。2005年6月，反对者增加到6个州政府和近400个地方政府。但是，无论在政界还是民间，很少出现对这个法案全盘否定的声音，分歧主要集中于某些敏感条款。[21]到2006年，参众两院重新审议《美国爱国者法案》时，为平息民怨，废止了这部法案中个别有争议的内容，但第215条等条款涉及的争议内容仍然保留了下来。

需要说明的是，从这个法案中获得“实惠”的中情局、联调局以及国安局等政府部门大都属于总统的管辖范围。获得“实惠”意味着地盘扩大、队伍扩大、预算扩大。

先说地盘，从“9·11”事件发生到2010年上半年，在华盛顿特区及其周边地区，有33座高度涉密的大楼新建或者在建，占地1700万平方英尺，相当于三栋五角大楼或者22个议会大厦的占地面积。中情局扩建了两座大楼，办公面积扩大了1/3。美国国家地理空间情报局（NGA，简称“地空情报局”）投资18亿美元新建了总部大楼。这么大规模的基础建设，在美国历史上并不多见。然后是人员队伍，仅以国防情报局为例，从2002年的7500人增加到2010年的16500人。再看看预算，2010年美国的情报预算达到750亿美元，是“9·11”事件之前的21.5倍。[25]

从某种意义上说，本·拉登领导的“基地”组织策划了“9·11”事件，最终搭上了“基地”组织很多人的性命，包括本·拉登自己，所以他们算不上赢家。真正的赢家是小布什。以美国人的牺牲，再加上全世界大多数人的同情，在与国会的权力争夺和与国民的权利争夺中，小布什没有太费

力就扩大了自己的权力和权利，打响了以“打击恐怖主义”为口号的漫长的战争。

---

1. 1平方英尺≈0.093平方米。——编者注

两场战争

普通人几乎是在一夜之间才知道“本·拉登”和“‘基地’组织”这两个名字的，其实他们在美国情报部门的黑名单上已经有好几年了。1998年，美国驻坦桑尼亚和肯尼亚使馆爆炸案发生后，美国人就已经将他们锁定为幕后元凶。前总统克林顿几年后到澳大利亚进行过一次访问。面对台下的听众，他回忆说：1998年12月，他差一点儿就干掉本·拉登，只是考虑到行动有可能殃及300名无辜的妇女儿童，才最终决定按兵不动。历史就是这样充满巧合，就在他讲完这段话之后几个小时，“9·11”事件发生了。不过，美国官方在后来发布的报告中称，之所以取消12月的这次行动，是因为本·拉登突然离开了房间，即使发动进攻也会毫无收获。美国人在半年后还策划了另外一次报复行动，而由于不同来源的情报相互矛盾，行动最终也被迫取消。[26]

2001年9月11日上午11点左右，恐怖袭击刚发生几个小时，国安局局长海顿接到了中央情报总监特内特打来的电话。

特内特：你那里有什么情报？

海顿：是“基地”组织干的。

特内特：你能肯定吗？

海顿：我们在“基地”组织的网站上发现他们在大肆庆祝胜利。[13]

那天晚些时候，特内特参加了总统召开的国家安全视频会议。会上，小布什突然问他，这次恐怖袭击是谁干的。特内特告诉他：在全世界的恐怖组织里，有能力实施如此协调默契的袭击的只有“基地”组织。情报部门还监听到这个组织里的很多人在恐怖袭击之后热烈庆祝胜利。小布什对特内特和在场的其他人说道：“把你们的耳朵都竖起来。本届政府的主要任务就是找到他们、抓住他们。”在那天的日记里，小布什还写了这么一句：“我们认为，（恐怖袭击的元凶）是奥萨马·本·拉登。”[3, 16]

三天后，美国国会通过一项决议，授权小布什“有权动用一切必要且适当的武力，对任何蓄意谋划、从事、授权、协助发生于2001年9月11

日的恐怖袭击的国家、组织、个人，以及为其提供庇护的组织和个人采取行动”。[17]9月16日下午，总统做出决定：向恐怖主义开战，第一个战场就是阿富汗。[27]在电视直播的参众两院联席会议上，他这样讲道：

美国人民在问：是谁袭击了我们的国家？我们搜集到的所有证据都指向了一个叫作“基地”的结构松散的恐怖组织……“基地”组织领导人在阿富汗影响深远，他们支持控制着这个国家大部分地区的塔利班政权……

我们的反恐战争从打击“基地”组织开始，但不会到此为止……

我们要调动我们掌握的各种资源，即我们所有的外交手段、情报工具、执法手段、经济影响，以及所有必需的战争武器，拆解并消灭全球恐怖网络……

我们（对于这次恐怖袭击）的回应将远远不只是迅速的反击和零星的打击。美国人民不应该指望只进行一场战斗（就取得胜利），这将是一场长期的战争，和我们看见过的都不一样：其中既有激烈的打击行动，通过电视就能看到，还有隐蔽的行动，即使成功也秘而不宣。[28]

其实，小布什讲得很明白，在他的“反恐战争”这个大包里，装进去的不仅仅是军事行动，还有各种各样秘密的情报行动。国安局在《美国爱国者法案》之前、甚至在“9·11”事件之前，就已经开展了许多秘密的情报监视活动，这些项目都趁着这个时机纷纷“转正”，贴上了“反恐”标签，合理合法地成为“反恐战争”的组成部分。[29]

当然，情报界还需要进行思想动员和组织准备。其主要方法不外乎沉痛反思失误、全面查找原因、制定整改措施。其中最有影响的一份文件就是“9·11”事件委员会提交的报告。所谓“9·11”事件委员会只是个俗称，它的全称是“对美国遭受恐怖主义袭击进行调查的国家委员会”。

2002年11月，“9·11”事件委员会成立，他们从外交、情报、移民、商业飞行以及恐怖组织资金流动等方面进行了细致调查，查阅了250多万页的材料，质询了1200多位证人，历时20个月，到2004年7月正式发布了一份近560页的报告。[30]

中国国内目前可以找到的至少有两个版本，一个是中国人民公安大

学出版社的版本，书名是"'9·11'委员会报告"；另一个是中央编译出版社的版本，书名是"揭秘'9·11'"。该报告专门用一节文字来分析美国情报圈子如何不适应冷战结束后反恐新形势的要求，如何在思想上不重视、在组织上无准备、在行动上无作为、在信息上不共享，相应的结论就是情报部门必须改革，要全面改革。只是"事后诸葛亮"地查找问题源头、分析原因可不够，给决策部门出谋划策是必要的，主要建议有三条：一是建立美国全国反恐中心，整体负责打击恐怖分子行动中的国内情报和对外情报工作；二是设立国家情报总监（DNI）及其办公室，统领全国情报工作；三是建立以网络为基础的情报信息共享系统。[31～33]

就在世界人民（特别是情报同人）被美国人的所谓情报失误吸引、猜度他们接下来要进行的情报改革时，美国却大张旗鼓地展开了进攻阿富汗的军事行动，一项极为秘密的情报监视行动也如影随形、悄然启动。这项监视行动打破了20世纪70年代以来，各个监督单位对情报部门"严防死守"的局面。

小布什的黑名单上还有两个名字：萨达姆（Saddam Hussein）和伊拉克。

据美国国家安全委员会的克拉克回忆，"9·11"事件后的第二天，小布什就在白宫召开会议，命令国家安全委员会着手调查"基地"组织和萨达姆有无联系。他说："我想让你们尽快再查一遍，全都再查一遍，看看是不是萨达姆干的，查清他和此事有没有联系……哪怕只有一丁点儿关联，也要查出来。"国家安全委员会后来报告说：查不到任何能将伊拉克与恐怖袭击联系起来的证据。结果这份报告一交上去，就被退了回来。尽管很多人并不相信小布什真的召开了这次会议，但有一点是肯定的：总统认为应当严肃考虑尽快打击伊拉克的问题。[34]

2001年9月18日，带有炭疽杆菌的邮件被投到美国的数家新闻媒体办公室和两位议员那里，造成5人死亡、17人被感染。接下来的调查过程虽然声势浩大，却虎头蛇尾、不了了之，使其成为一桩疑案。联调局甚至专门为这桩案子创造了一个新词"Amerithrax"。折腾了8年多时间，到2010年2月，联调局才正式结案。尽管缺少直接证据，但他们还是把一个名叫布鲁斯·艾文斯（Bruce E.Ivins）的嫌疑人定为元凶，不过此人已在结案前的2008年7月自杀身亡。[35]美国国家科学院（NAS）事后对联调局的调查过程进行了评估，对其最终确定的元凶表示怀疑。[36]这些都是多年以后的事情了。在2001年的那个多事之秋，"9·11"事

件再加上炭疽疑云，闹得全美上下人心惶惶。

利用这次炭疽恐慌，小布什把大规模杀伤性武器也纳入了“恐怖主义”的范畴，然后顺理成章地把寻找这类武器作为战争的一项内容。在当时的形势之下，谁要是搞大规模杀伤性武器，那就可以让全美人民共讨之、全世界人民共伐之。2001年11月，小布什总统命令国防部着手规划伊拉克战争，事实上，美军中央司令部在此之前已经接到命令，把打击伊拉克的战争前景分析清楚。[34]

小布什知道，要让普通百姓支持对伊拉克作战，彻底拔掉萨达姆这根“钉子”，必须把萨达姆和大规模杀伤性武器联系在一起。带着这种先入为主的认识，他耐心地等待着时机。

戴维·凯（David　Kay）本科毕业于得克萨斯大学奥斯汀分校，后来在哥伦比亚大学获得硕士和博士学位，先后在联合国教科文组织（UNESCO）和国际原子能机构（IAEA）建立技术援助项目的评估部门工作，1991～1992年担任联合国对伊拉克核武器核查小组的首席官员，之后长期担任科学应用国际公司（SAIC，简称“科应公司”）的副总裁。[37]2002年9月，戴维·凯面对《美国新闻与世界报道》的记者，拍着胸脯说：“伊拉克明显违背了国际法，他们没有完全销毁大规模杀伤性武器。”[38]

2002年10月，那份“著名”的、有关伊拉克的《国家情报评估报告》出炉，报告的题目是“伊拉克的大规模杀伤性武器计划还在进行中”。[39]

报告言之凿凿地宣称萨达姆重建了他的导弹和生物武器设施，并且试图用民用生产的幌子掩盖他扩张生化能力的事实。报告还危言耸听地警告说，伊拉克有一个“无人机计划”，可以用来投放生化制剂，这对它的邻国、驻扎波斯湾的美军，甚至美国本土都将造成严重威胁。在报告的结尾，列出了以下几点结论，并且标上了“高度可信”。

伊拉克正在继续实施、某种程度上还在扩张其化学、生物、核弹与导弹计划，违反了联合国决议。

伊拉克拥有被禁止的生化武器和导弹。

一旦得到足够的武器级裂变材料，伊拉克将在几个月到一年内制造

出核武器。[39]

小布什心里还是没底儿。12月21日，他找来了中央情报总监特内特等人。

小布什：我想，普通民众理解不了这些情报，也得不到太多信心。……这就是我们得到的最有力的情报吗？

特内特：这已经是一次“强力灌篮”[注]了！

小布什：你对这件事有多大把握？

特内特：不用担心，这回真的是“强力灌篮”了！[40, 41]

看来喜欢拍胸脯的不止戴维·凯一个人，特内特从此为自己赢得了“灌篮总监”的称号。

很多人会把“中央情报总监”（DCI）和“中央情报局局长”（D/CIA）混为一谈——不少美国人也是如此。中央情报总监这个职位在中情局成立之前一年就有了。设立这个职位的主要目的就是协调美国国内情报力量，为决策者提供更好的服务。但由于中央情报总监同时被赋予了中情局最高管理者的职能，而要把这么大的单位运转起来，本身就是一件工作量巨大、工作难度也不小的事情。美国情报界的各方力量缺乏有力统管和有效协调，“山头主义”问题也很严重，这个问题并没有因为设立了中央情报总监一职而得到太多改善，甚至逐渐变成了一道“难题”。中央情报总监的命令多半也只在中情局内部才算数，他们没有也不可能发挥好协调作用，历任总监的主要精力都放在中情局的工作上，成为事实上的“中央情报局局长”。[42]对局外人而言，“中央情报总监”和“中央情报局局长”这两个头衔的名称又太接近、太容易混淆。所以，人们搞不清楚也是情有可原的。

前面提到“9·11”事件委员会建议设立国家情报总监一职，实际上就是把“中央情报总监”的职能一分为二，统管和协调等工作由国家情报总监负责，管理中情局这件事情则让中情局局长专心去干。2004年9月，按照《2004年情报改革和反恐法案》的要求，第19任、也是最后一任中央情报总监波特·戈斯（Porter Goss）改任新一任中情局局长，他原先承担的统管和协调美国15家情报单位的任务，以及向总统汇报的任务，统统交给了第一任国家情报总监约翰·尼葛洛庞帝（John Negroponte）。8

月16日，戈斯举办了一个小型派对，邀请8位前中央情报总监，包括老布什（George H.Bush），回到中情局总部，畅谈中央情报总监曾经做出的贡献。可惜新任国家情报总监没有参加这次活动。[43]这是后话了。

为了让大家相信最危险的“坏蛋”是萨达姆，美国政府积极行动起来，与新闻媒体联手进行舆论“轰炸”。国家安全委员会里有一群高级官员专门负责向公众宣传萨达姆的威胁，包括康多莉扎·赖斯、副总统的国家安全事务助理利比（Lewis “Scooter” Libby）等，他们尤其强调伊拉克在短期内可能带来的核威胁。小布什还曾单独给赖斯和幕僚长卡德下命令，要他们想办法提高普通民众对即将到来的战争的支持率。[34]有了这些铺垫，攻打伊拉克的时机终于到了。就在这时，受联合国的派遣进入伊拉克的一个武器核查小组，面对联合国安理会，汇报了过去几个月的调查结果，时间是2003年1月27日，他们宣称：

我们尚未发现伊拉克恢复其自20世纪90年代消除的核武器方案。……现在我们的核查系统已经就绪，除非发生特殊情况，并且只要伊拉克提供持久积极的合作，我们应该能够在数月内提供关于伊拉克没有核武器方案的可信保证。我认为，这几个月应该是对和平的有价值的投资，因为它们可以帮助我们避免一场战争。[44]

尽管联合国小组说最好再等几个月，没准儿可以避免一场战争，但小布什决定不再等待。一声令下，打！接下来，萨达姆被生擒，世界人民都看到这位伊拉克总统的狼狈不堪和悲惨结局。但让所有美国人大跌眼镜的是，伊拉克被查了个底儿朝天，大规模杀伤性武器也没能被找到。

事情变得有点儿复杂了。

---

1. slam-dunk，相当于我们常说的板上钉钉。

“我们全都错了”

戴维·凯说：“这句话很可能被刻到我的墓碑上。”[37]

从伊拉克时间2003年3月20日美英联军的“斩首行动”和“震慑行动”开始，到4月15日联军宣布主要军事行动结束，美军共死亡262人，其中阵亡139人、事故死亡123人，总花费达230亿美元。除了肉体的伤害之外，由于作战环境陌生，美国士兵心理压力极大，整日感到草木皆兵，不少人回国后还深受心理疾患的困扰。[45, 46]想想也能理解。相比于伊拉克战场，美国国内的条件无疑是优越的、生活是安逸的、精神上是放松的，这种巨大落差让年轻的小伙子们去承受，有些不适应也难免。费了这么大劲儿、遭了这么大罪，目的很明确，就是要找到大规模杀伤性武器、拯救世界，使其免遭毁灭。美国大片里坚持宣扬的都是这种拯救世界、舍我其谁的勇气和情怀。大规模杀伤性武器要是真的落入萨达姆或者“基地”组织手里，世界就真的不太平了。

仗打完了，打得还挺好，打仗的理由却迟迟没有落实。所以，这边战火刚平息，以美国人近乎完美的军事胜利宣告结束，那边就已经有几支队伍开始寻找大规模杀伤性武器了。2003年5月，又一支队伍进入了伊拉克，这个专门成立的伊拉克调查小组（ISG）有1400名成员，分别来自美国、英国、澳大利亚三国，说它“浩浩荡荡”一点儿也不夸张。他们接替了此前一无所获的“第75搜寻别动队”。戴维·凯自然成为领导这个调查小组的最佳人选。他们此行的目的只有一个：掘地三尺也要找到大规模杀伤性武器。[47, 48]

戴维·凯知道，他的压力极大，调查小组必须紧锣密鼓地开展工作。

2003年5月底，核查小组在伊拉克境内“发现”了萨达姆的移动生化武器实验室。这一“重大发现”当然需要由小布什总统亲自宣布。美国媒体一片欢呼雀跃。后来的调查结果却是，这个“发现”有造假的嫌疑，所谓的移动实验室不过是两辆卡车。更让人生气的是，在小布什向世人宣布这个“发现”的前两天，9位专家就已经写好了一份报告，他们想告诉总统这两辆车跟化学武器没有丝毫关系。可是，上级部门只是在这份报告上盖了一个“机密”的印戳就把它锁进了柜子。在此之后一年的时间

里，政府和情报官员坚持对所有人说：它们就是武器实验室。[49, 50]

调查小组对伊拉克境内的每个可疑地点都进行了地毯式的全面搜寻，对每个与大规模杀伤性武器计划有关的人员也进行了调查和询问，但是仍旧一无所获。[51]于是，戏剧性的一幕发生了。2004年1月，戴维·凯提出辞职。原因很简单，他干不下去了。他告诉路透社："我认为它们不存在。"[52]紧接着，他硬着头皮对参议院武装力量委员会说：

我想以这样一句话开始，几乎所有人都错了，其中包括我自己……在战前，我的看法是，我看到过有力的证据，证实伊拉克的确拥有大规模杀伤性武器……现在，根据我个人的判断，我们全都错了。这是最让人不安的事情。[53, 54]

媒体评论他的离职原因时用了一个词——"幻想破灭"。[52]

调查小组在新组长查尔斯·迪尔费尔（Charles Duelfer）的领导下，终于在2004年9月拿出了一份调查报告，又称"迪尔费尔报告"。这份长达1500页的报告绕来绕去、冗长啰唆，归结起来其实就是一句话：萨达姆没有制造大规模杀伤性武器的计划。尽管很不情愿，但报告还是在最后的附录里，对一年前"发现"的移动实验室给出了一个明确说法：那只不过是伊拉克共和国卫队用来为无线电探空气球充气的氢气发生装置。当然，这份报告还是不忘给萨达姆泼上一盆"脏水"，说"如果联合国解除了制裁，萨达姆对于开展大规模杀伤性武器计划还是有想法的"[55]等。

这是多么残酷的事实：伊拉克没有大规模杀伤性武器，并且萨达姆与激进的"基地"组织也没有什么联系。那为什么要去打仗呢？最终，总要有个说法。首先是美国士兵不答应，然后是美国人民不答应，国会那里也绕过不去。

小布什嘴上迟迟不肯认错，不过他的心里早就开始思考这样一个问题了：谁来当替罪羊？

戴维·凯辞职后不久，小布什就发布了第13328号总统令，宣布成立一个独立调查委员会来审查对伊作战的情报失误问题。这个调查委员会是按照总统令建立的，委员会成员由小布什任命，对他负责，向他汇报，其工作日程和提交报告的日期也由小布什决定，总之，小布什对这个委员会拥有主导权。[56]独立调查委员会是小布什布下的一个棋子，其根本任务就是撇清他自己对伊战的责任、掩护他全身而退，所以调查

范围、调查结果难说公允，该调查从一开始就“先天不足”。为了减轻压力，小布什把这个委员会的工作范围扩大到整个大规模杀伤性武器的情报工作，最终拿出来的报告将不只检讨伊拉克的事情，还检讨了利比亚、伊朗、朝鲜和“基地”组织等国家和组织的“大规模杀伤性武器”问题。[57]这样一来，对伊作战情报失误的主题自然就被冲淡了。几乎同时，小布什的好伙伴、英国首相布莱尔也宣布要成立一个类似的委员会审查英国情报界的问题。

转眼到了2005年3月底，调查委员会拿出了一份近700页的报告，对外公开的则有601页。在报告正文之前，有一封给总统的信件，信中“沉痛”宣布：情报界在战前，对伊拉克大规模杀伤性武器的判断“几乎全都大错特错”，“这是一次重大的情报失误”。不仅评估结论错误，形成评估结论的方法，以及情报部门与决策者交流的方式等都有严重的缺陷。[58, 59]

报告深刻剖析了错误根源，提出未来防范失误的方法在于深化改革，建立一个真正完整、更有想象力、愿意采用新技术的情报系统。报告建议赋予国家情报总监更实在的权力，使得这个职位的负责人能够更好地处理中情局、国防部和其他情报部门对其权威的挑战。报告还呼吁对联调局和中情局进行广泛的改革。看来，美国的情报改革只有进行时，没有完成时。[59]

报告还说，在伊拉克战争前，中情局向小布什提供的《总统每日简报》（PDB）有问题，简报通过吸引眼球的标题和不断重复那些并不确凿的资料，无形中“放大”了对伊拉克重建大规模杀伤性武器的判断。报告把情报失误的责任直接归咎于情报部门，但同时又扭扭捏捏地承认：没有发现情报机构故意歪曲有关伊拉克存在大规模杀伤性武器的证据。[59]

报告林林总总地提出了74条建议，小布什采纳了其中的69条。算上2004年7月的“9·11”事件委员会的调查报告，这是美国在一年之内出炉的第二份涉及情报改革的报告了。看来每隔一段时间，情报工作就会被拿出来顶罪说事，原本很认真地看待美国人“情报改革”的那些人，现在是不是可以稍微看淡一些他们所谓的“改革”呢？

2008年11月30日，小布什就要离开白宫了。面对记者，他装模作样地说，作为美国总统，自己最后悔的一件事情就是误信了萨达姆拥有

大规模杀伤性武器的不正确情报，发动了伊拉克战争。他甚至说："我多么希望当时得到的情报不是这样的。"[60]小布什把自己的责任推卸得一干二净，背黑锅的只剩下情报部门。

就在调查委员会的工作启动后不久，2004年6月，"灌篮"总监特内特就宣布辞职。原因？当然是"为了家庭的幸福"等"个人原因"。[61]除了这些似曾相识的老套说法，特内特没有其他选择。他是克林顿总统任内的中央情报总监，小布什上台后没有依据"惯例"换掉他，当时还曾引起民间的种种猜疑。其中一种说法是，特内特把中情局总部大楼命名为"乔治·布什情报中心"有谄媚之嫌。这里的"乔治·布什"指的是老布什，他曾经在1976～1977年当过近一年的中央情报总监。特内特这么做，自然会让人产生一些联想。然而，大楼命名是在1999年，特内特肯定预见不到两年之后小布什将子承父业、成为美国总统，所以这种说法未必站得住脚。把当事人、"老领导"，同时也是前总统的老布什请回中情局参加命名典礼，一点儿也不过分。不过，通过这件小事，特内特实实在在地从布什家族那里得到了感情加分，这也在情理之中。再加上老布什一直认为中央情报总监这个位置并不需要跟总统任期直接挂钩，他自己当年就没有换掉前任总统设立的中央情报总监。[62]所以，当小布什为了组阁向他询问中央情报总监人选的时候，他告诉自己的儿子：特内特非常受人尊敬。[63]

对于特内特的"忠心耿耿"，小布什心里比谁都清楚。但发生了这次伊拉克的事情后，面对日趋临近的第二任总统选举，小布什只能忍痛割爱，让特内特来当这只背黑锅的"替罪羊"。

几个月后，他特意主持了一个授勋仪式，为这位"灌篮"总监以及曾经分别主持伊拉克军政大局的汤米·弗兰克斯（Tommy Franks）和保罗·布雷默（Paul Bremer）这三位伊战"功臣"颁发总统自由勋章，算是给了特内特一点儿小小的心理安慰。[64]

2008年，特内特出版了自己的回忆录《风暴中心》（*At the Center of the Storm*），对当年那次自己荣获"灌篮"称号的会议专门进行了辩解。他的解释归纳起来只有一句话：这次御前会议跟小布什下决心出兵伊拉克压根儿没什么关系。因为早在会议之前10个月，也就是2002年2月，总统就已经看过第一版对伊作战计划了，而在那次会议前半个月，五角大楼就已经下达出兵的命令了。[65]

特内特显然忘了，在更早的2001年12月28日，他参加过一次国家安全委员会的视频会议，弗兰克斯将军和总统在得克萨斯州的农场，国防部长在他新墨西哥州的家中，科林·鲍威尔（Colin Powell）、康多莉扎·赖斯和特内特则在白宫参加了这次会议。在这次会上，弗兰克斯简要汇报了对伊拉克作战计划的准备情况，当时的计划几乎照搬了1991年海湾战争的方案。弗兰克斯提出要重新拟订一份新的作战计划。在怀俄明州的家中参加会议的副总统理查德·切尼（Richard Cheney）后来在回忆录里讲述了这次会议的情况，他甚至还清楚地记得，对伊拉克作战计划的代号是“第1003号方案”。[66]

特内特在接受《60分钟》节目采访时说，副总统切尼在媒体上渲染“灌篮”会议，意在给人一种印象，总统似乎需要他的“灌篮”才能决定出兵伊拉克，实际上并非如此。[67]

看来，从“灌篮”故事开始在民间流传的那一刻起，特内特就被当成一枚背黑锅的棋子了。现在他突然想洗脱加在自己身上的“错误”，自然就引起了来自各方的讽刺、鄙视和攻讦。

在小布什心里，对于伊拉克战争，还有一个人必须负责任。这个“倒霉蛋”，哦，不，更准确地说，是“眼中钉”，必须要解决掉，他就是伊拉克总统萨达姆。

萨达姆的社交网络

时间又回到2003年。

5月1日，随着一架S-3舰载反潜机被“亚伯拉罕·林肯”号航母的阻拦索稳稳地拦下，小布什总统又创造了一个“第一”：成为第一个尝试利用航母阻拦装置着舰的美国总统。[68]不过也有人说这没有必要：因为航母就在他的直升机的飞行半径以内，他完全可以坐他的专机降落在航母上，这种刻意的安排比例行的安排要多不少花销。[69]别的不说，针对可能发生的意外，就要专门给总统安排若干次水中逃生的模拟训练，而这些都是要花钱的。[70]美国人其实还是有点儿小家子气，总统也不是天天心血来潮、弄出新花样，难得他要显摆一下，破费一点儿算得了什么，再说他这么做对提升士气也有一定帮助。

航母上早已拉起了巨型彩色横幅，上面写着“任务完成”。小布什身穿绿色飞行服、提着闪闪发亮的飞行头盔，神气地走出了机舱，和舰上兴奋的年轻士兵们合影留念，非正式地检阅了刚从战场凯旋的官兵。几个小时后，他换上了西装，站在摄像机前，神采飞扬地发表演说。一上来，他就高声宣布：“在伊拉克的主要军事行动结束了。”[71]

一番热闹之余，美国人想起了两件事情，一是大规模杀伤性武器还没有找到，二是伊拉克总统萨达姆还没有抓到。这时大家才恍然大悟，原来这是小布什在作秀以转移公众的关注焦点啊！伊拉克的抵抗运动一点儿也没有消停的意思，美军的伤亡人数几乎每天都在增加。“任务完成”？只当是个笑话吧！小布什后来也承认，这种宣传落下一个被人批评的笑柄，“是一个巨大的错误”。[72]

再说萨达姆。他仓皇逃回了故乡提克里特，在那里遥控伊拉克的抵抗运动。一开始，美军以为他们遇到的抵抗是无组织的，后来才发现这些抵抗是有组织、有策划的。[73]美国人对他们的敌人毫不留情地使用一些明显具有贬义且肮脏不堪的字眼。比如，他们把伊拉克境内各种各样的抵抗行动统称为“叛乱”，把抓住的俘虏统称为“囚犯”，还额外赠送给萨达姆一个外号，叫他“巴格达的屠夫”。这些说法后来便一直沿用下来。

在对伊作战期间，美军别出心裁地把伊方“战犯”按照他们理解的重要程度，编成了一套扑克牌，把通缉令这样一种枯燥的东西转变为士兵喜闻乐见的形式。当然，邪恶的黑桃A非萨达姆莫属，其他的牌则是他的政府高官们。中国人常说“打扑克”或者“打牌”，美国人则叫“玩扑克”或者“玩牌”，不管是“打”还是“玩”，这套伊拉克战犯扑克牌的发明，已经让美军在口头上占了一个很大的便宜，心理上也已经先胜一筹。

在小布什发表“任务完成”的演说之时，扑克牌高官中已有12个或者投降，或者被俘，在接下来的一个月时间里，又抓住了12个。但美军发现，抓住这些大人物并未给他们追捕萨达姆带来什么有用的线索[73]，因为萨达姆并没有把自己的行踪透露给这些政府高官，他并非不信任他们，只是此时此境，他更信任另外一些人。

这其中最典型的例子是阿比德·哈米德·马哈茂德·提克里蒂（Abid Hamid Mahmoud al-Tikriti），在萨达姆当政期间，他是总统的私人秘书。萨达姆走到哪里，阿比德就跟到哪里，外界认为他极受萨达姆信任，他被视作“萨达姆的影子”。在扑克牌里，他是方片A，可见在美军眼里他的重要程度。所以，当他在6月中旬被擒获时，美国国内一片欢呼，以为拿下萨达姆指日可待。可是美国人很快就失望了：阿比德已经有一阵子没有跟萨达姆在一起了，也根本不知道萨达姆的下落。[73]看来，萨达姆采取的策略是：大厦将倾，大家各奔东西、好自为之。

曾经担任过中情局人格与政治行为分析中心负责人的杰罗德·珀斯特（Jerrold Post）认为：萨达姆本人非常熟悉和喜欢美国电影《教父》，他从这部电影里学到了这样一个“道理”：危急时刻，人们应该转向他的族群寻求信任和支持。[73]珀斯特拿《教父》说事儿，他的潜台词也是明显的：萨达姆就是一个黑社会头领。当然，萨达姆抛弃了他的政府，丢下了他的正规军，另外组建了一支“萨”家军来做最后的抵抗，这也的确让他的对手抓住了口实。他这种弃师潜遁、狼狈出逃，从一国领袖迅速沦为流亡者的形象，实在没有办法跟临危不乱不惧、至死不离开总统府一步的智利前总统萨尔瓦多·阿连德（Salvador Allende）相提并论。

在他的家乡提克里特，萨达姆有他的铁杆支持者——“五大家族”：哈桑家族（Hasans）、马吉德家族（Majids）、穆斯里特家族（Musslits）、哈杜希家族（Hadooshis）和赫拉莫斯家族（Heremoses）。这些家族里的成员基本上都没有出现在扑克牌上。[73]

美军在这一地区部署了两股力量：一股是规模很小的特别行动队，其主要任务是追捕要犯；另一股是第四步兵师第一旅战斗队，其主要任务是维持当地的社会稳定和秩序。[73]两股力量在抓捕萨达姆过程中的大致分工是，旅战斗队负责袭击、抓人，特别行动队负责审讯俘虏，为旅战斗队提供袭击线索。

埃里克·马多克斯（Eric　Maddox）是特别行动队的成员，同时也是中情局的分析人员。经过几个月高强度的审讯工作，他逐渐认识到，要抓住萨达姆，应该把提克里特的一些行事比较低调的伊拉克人作为重点突破口。可他的上级领导不这么想，他们认为要抓住萨达姆，应该从扑克牌上的那些大人物身上找突破口。[74]

“社交网络分析”对普通人来说是个新鲜词语，可对中情局的分析人员而言，却是一门必须熟练掌握的基本功。为了完成任务，马多克斯必须要画出目标人物之间的关系图。由于和领导意见不一致，他想出了一种蒙混过关的办法：做两张不同的萨达姆社交网络图，一张给领导看，把某些扑克牌上的大人物放上去；另一张留给自己用，上面列的是另外一些人。不久，马多克斯得到了一份萨达姆的保镖名单，其中有40多个人来自提克里特的穆斯里特家族。[74]这对他分析萨达姆的社交网络帮助很大。

马多克斯审讯战俘的方法很特别，他极少进行暴力审讯，也几乎不问“叛乱”的情况，而是问“你平时都跟谁一起喝酒”、“跟谁一起钓鱼”这样的问题。战俘们不明就里，便落入了他的圈套，“配合”得很好。随着审讯工作的深入，萨达姆的社交网络越来越清晰，来自穆斯里特家族的路德曼和穆罕默德两兄弟成为最终找到他的关键。严格说起来，他们这一家人还算是萨达姆母亲那一边的亲戚，兄弟俩都曾当过萨达姆的私人保镖。[74]11月8日路德曼被俘，审讯还没开始，他就因心脏病突发而猝死。马多克斯发现，路德曼的被俘和死亡并没有对当地的“叛乱”产生任何影响，这就说明原来的判断还不准确，真正关键的人物只剩下一个：穆罕默德。[75]由于叫“穆罕默德”的人实在太多，因此有必要把穆斯里特家族里的这个“穆罕默德”的全名说一下，穆罕默德·易卜拉辛·奥马尔·阿·穆斯里特（Mohammad　Ibrahim　Omar　al-Musslit），美军根据一张模模糊糊的照片，把他叫作“肥仔”。[74]

根据战俘的口供，美军袭击了一个养鱼场，抓住了两个钓鱼者，他们神情紧张、神色慌张。这时，留给马多克斯的时间也不多了——他必

须按规定在一周任期结束后马上回国，他能做的只有争分夺秒、加快审讯步伐。一番讯问过后，他们了解到其中一个钓鱼者是“肥仔”的钓鱼密友穆罕默德·胡达伊尔（Mohammed Khudayr）的表兄弟。顺着这条线索，美军包围了巴格达的一处房屋，抓住了四个人，胡达伊尔本人就在其中。马多克斯抓紧时间开始审讯，此时距离他的航班起飞只剩下6个小时。[75]一番较量之后，胡达依尔终于开口了。

胡达依尔：我确实认识穆罕默德·易卜拉辛。

马多克斯：他昨晚在哪里？

胡达依尔：他就在那个房子里。

马多克斯：我们还是让他跑掉了。

翻译：不，他是说，他就在那个房子里。[76]

马多克斯激动得快要疯了！他跑到牢房，把剩下三个人的头巾都摘掉。“肥仔”果然在里面。

马多克斯：你就是穆罕默德·易卜拉辛吧。我在此等候多时了。

……

翻译：他说，他也等候你多时了。[76]

两个小时之后，“肥仔”对马多克斯说：我带你们去找他——他就是萨达姆。时间容不得半点儿耽搁。美军带着“肥仔”飞回提克里特，他们来到了阿道尔镇。这个小镇对于萨达姆的意义非同一般。1959年他密谋暗杀总理未遂，一路潜逃来到阿道尔镇，从这里游过了底格里斯河，逃到了叙利亚。等到自己执掌政权之后，为了纪念那次顺利逃亡，萨达姆每年都要来这里游一次泳。[75]

几个小时之后，美军在小镇边上的一个农场抓到了一名男子，他蜷缩在一个地下洞穴里，满脸胡须，狼狈不堪，按美军的说法是“像只大耗子”。此人正是伊拉克总统萨达姆。[77]这一天是2003年12月13日。

昔日的荣华富贵已如过眼云烟，此时的萨达姆已经家破人亡，成为真正意义上的丧家之犬、孤家寡人。他的两个儿子乌代（Uday）和库赛

（Qusay），连同他14岁的孙子穆斯塔法（Mustapha），都在几个月前的一场战斗中死去。[78, 79]

马多克斯回国后不久，因为他在抓捕萨达姆过程中的突出贡献，得到了国防部部长唐纳德·拉姆斯菲尔德（Donald Rumsfeld）和中央情报总监特内特的接见，并且获得了一枚荣誉勋章。[75]后来他根据自己在伊拉克的这段经历写成了一部回忆录，题目就是“任务：黑名单1号”（*Misson: Black List #1*）。多年以后，在接受记者采访时，他仍然可以凭着记忆画出萨达姆的社交网络图。[75]

上面只说了特别行动队方面的事情。其实，提克里特另外的那支美军部队也使用了社交网络分析技术。这支旅战斗队的指挥官是詹姆斯·海基（James Hickey）上校，他早年毕业于弗吉尼亚军事学院。[80]海基手下有一员干将，行动指挥官布莱恩·瑞德（Brian Reed）少校。他在西点军校上学时接触过网络理论，后来拿到了社会学硕士学位，对这套社交网络分析方法颇为熟悉。[81]他的这些专业基础知识，在抓捕萨达姆的过程中派上了用场——海基上校到任后不久就命令情报官绘制战俘和目标人物的关系图。[73]打仗抓俘虏这样的事情，瑞德未必十分突出，但要说到把社交网络图中的重要节点（也就是关键人物）计算出来，他可以说是驾轻就熟，这一点在海基的部队里十分难得——要知道计算能力是很多美国人欠缺的一项本领。于是，海基让瑞德和情报官共同绘制萨达姆的社交网络图。在他们绘制的图上，“肥仔”是连接萨达姆和穆斯里特家族的关键节点，而他的兄弟路德曼，因为被视作抵抗运动的主谋，也成为图上的一个重要节点。[74]海基上校的部队有一个与众不同的“习惯”：每次袭击行动完成之后，他们会把房屋里所有的家庭成员的照片、合影仔细收集起来。原因很简单：这些照片能帮助他们绘制社交网络图。[81]

回国后，瑞德以萨达姆的社交网络为主题，完成了他的社会学博士论文，题目就是“非正式网络的形式化：对叛乱的网络分析”（*Formalizing The Informal: A Network Analysis of An Insurgency*）。关于萨达姆的社交网络，他的结论是这样的：萨达姆有一个节点分布比较稀疏的大社交网络，但与他有直接联系的核心网络规模很小。在总节点数为214个的大社交网络中，直接连接萨达姆的节点只有22个。这22个节点构成了一个以萨达姆为中心的核心网络，节点间的联系主要是家族和部族关系，并且连接得非常紧密。[82]

事后，参议院情报委员会主席帕特·罗伯茨（Pat Roberts）评论说："抓获萨达姆是情报分析人员、行动组人员和军队大力协同、通力合作的直接结果。"[83]他的这句话比较中肯、恰如其分。

三年之后的2006年12月30日，在伊拉克当了近24年总统的萨达姆，在他自己的国家被自己的同胞送上了绞刑架。小布什事后发表了一份声明，对这个"倒霉蛋"的下场冷嘲热讽了一番。他说，在萨达姆执政期间，他对自己的人民犯下滔天罪行，人民最终对他进行了公正的审判；这是伊拉克通向民主进程中的一个重要里程碑，从此，伊拉克成为美国反恐战争的同盟军。[84]法庭历数了萨达姆的"五大罪状"，主要包括：入侵科威特、对什叶派穆斯林进行政治迫害、对库尔德人进行种族清洗、破坏沼泽阿拉伯人的生活资源、杀害政治对手。[85]

萨达姆当政多年、大权独揽，必定做了不少坏事、结下了不少仇怨，更何况伊拉克原本就是一个民族矛盾尖锐、宗教冲突严重的地区。他从总统的位置跌落下来变成战犯，再变成罪犯，因此伺机而动想要公报私仇、落井下石、借刀杀人的人恐怕为数不少。审判是否公正，历史自有公论。对这场受到美国影响的审判，小布什当然要冠以"公正"一词，其潜台词就是，萨达姆竟敢跟我们唱对台戏，敢跟我们捣乱，最后一定要让你死得明白，谁才是这里真正的"老大"，这就是你应得的"公正"。

但所谓"同盟军"，也就是对美军俯首帖耳而已。如果希望被扶持起来的伊拉克政府对反恐战争出钱出力，那是根本不可能的。因为战后的伊拉克是一个十足的泥潭，经济崩溃，社会动荡，政府风雨飘摇。把他们称为"同盟军"，美国纯属打肿脸充胖子。不过，小布什在声明中说，萨达姆的死并不能结束那里正在发生的暴力活动。[84]这话倒是真的。

小布什已经没有时间收拾伊拉克这个烂摊子了，踌躇满志的巴拉克·奥巴马（Barack Obama II）则把从伊拉克撤军作为竞选总统时的一条主要承诺。上任伊始，奥巴马就要求负责伊拉克战争的美军中央司令部制定从当地撤军的具体时间表。[86]2011年10月22日，奥巴马宣布，驻伊美军将于年底前全部撤出。两个月后，美国最后一批驻伊部队跨过伊拉克边界进入科威特。至此，伊拉克战争画上句号。在8年的战争中，共有4487名美军士兵丧生，但其中只有262人死于大规模军事行动，其余绝大多数人都是在无谓的消耗战中殒命的。战争的另一方呢？有超过11万名伊拉克人丧生，160万伊拉克人流离失所。这场战争显然极不对

等。[87, 88]

奥巴马对自己把美军拉出泥潭颇为得意。他对一批又一批听众说：“我结束了伊拉克战争。”但他说的只是小布什发动的伊拉克战争，伊拉克国土上此后再无宁日。美军撤出后形成的真空留给了“基地”组织这样的伊斯兰极端势力。美军前脚一走，他们后脚跟上、乘虚而入。2014年1月，在安巴尔省重镇费卢杰，“基地”组织打败了当地的安全部队，全面占领了这座城市。提到费卢杰，小布什心中应该会隐隐作痛，因为美军在这里进行过一场攻坚战，那是整个伊拉克战争中最艰苦的一次战斗。不知道当他看到“基地”组织的旗帜在费卢杰市政府大楼上升起时，心中做何感想。[89]但这样的景象，情报界在对伊作战前就已经预见到，并且已经告诉他了。他们是这样说的：

伊拉克（国家）不可能分裂，但日后萨达姆政府将很可能面对一个深度分裂的社会，国内的不同势力将卷入暴力冲突，除非有一个占领力量阻止他们这么做。……如果巴格达控制不了伊拉克农村，“基地”组织或者其他势力就会乘虚而入。[90]

“基地”组织很可能在伊拉克战争期间或者战后加快他们的行动节奏，增加恐怖袭击的次数。……伊拉克境内的好战者得到的资金和支持可能增加，他们会对驻伊美军进行恐怖袭击。……美国打败并占领伊拉克，伊斯兰政治化的支持者可能大幅增加。[91]

这些话出现在美国国家情报委员会递交给白宫的两份《情报界评估报告》（ICA）里，在政府高层被广泛传阅，时间是2003年1月，也就是伊拉克战争爆发前两个月。[92]小布什应该没有忘记。

把萨达姆作为拥有大规模杀伤性武器的恐怖分子，从而把伊拉克作为反恐战争的一个战场，这是小布什借助虚假情报甚至是操控情报，为美国人民、伊拉克人民准备的一枚苦果。“9·11”事件的主谋本·拉登倒真的是一个彻头彻尾的恐怖分子，对他进行追踪、猎杀是可以为反恐战争扳回一分的。这个时刻终于到了。

头号功臣

当地时间2011年5月2日。

凌晨1点刚过，月黑风高，巴基斯坦伊斯兰堡附近的阿伯塔巴德镇，人们已沉入梦乡。美军海豹突击队员潜入镇上一处神秘的院落，与院里的人交了火。40分钟后，战斗结束。“9·11”事件之后终日东躲西藏的本·拉登被击毙，他的尸体被突击队员运上直升机，验明正身之后进行了海葬。[93]

这场战斗给世人留下深刻印象的首先是海豹突击队的神勇，但其实他们并非百战百胜，比如说在索马里，他们在那里曾经多次折戟。其次给人留下深刻印象的是一张照片：奥巴马神情严肃，带着他的高级幕僚们，在几千公里外的白宫战情室，透过电视屏幕观看战斗实况。战斗由坐在他身边的空军准将马歇尔·韦布（Marshall Webb）直接指挥。[94]这就是“决胜千里之外”。这张由白宫御用摄影师皮特·苏扎（Pete Souza）拍摄的照片，编号为“P050111PS-0475”，被上传到了Flickr的白宫网页上，一时间引发无数人无数次地转载、转载再转载，从而成为经典。

行动结束后不过几个小时，奥巴马就急不可耐地向全世界报捷：

……美国已经完成了消灭“基地”组织头目本·拉登的行动，此人是屠杀数以千计无辜男女老少的恐怖分子。

……

在过去10年中，得益于我们的军队和专业反恐人员不知疲倦的英勇工作，我们在打击“基地”组织方面取得了巨大进展。我们挫败了多起恐怖袭击，强化了本土安全。

……

我就任美国总统后不久，就曾命令中央情报局局长莱昂·帕内塔（Leon Panetta）把击毙或者抓捕本·拉登作为打击“基地”组织的首要任务……去年8月，在我们的情报部门历经数年的艰苦工作之后，我获悉

已经有了本·拉登的线索，尽管那时还无法确定。我们花费了数月才得以顺藤摸瓜找到他。我多次同国家安全人员会谈，也有更多信息锁定本·拉登就藏在巴基斯坦的一座建筑内。终于在上周，在我们掌握了充分的情报之后，我下令对奥萨马·本·拉登采取行动，将他绳之以法。今天，在我的指示下，美军对巴基斯坦阿伯塔巴德的一处目标实施了针对性的行动……双方交火后，美国士兵击毙了奥萨马·本·拉登，并且带走了本·拉登的尸体。

……

本·拉登之死是我们在打击“基地”组织的努力过程中，迄今为止取得的最为重要的成就。

……

这个晚上，让我们对那些因“基地”组织恐怖分子而失去亲人至爱的家庭说，正义终于得到了伸张。我们要感谢那些情报和反恐界的专业人士，正是他们孜孜不倦的工作才促成了今天的胜利。美国人民看不到他们的工作，也不知道他们的名字。[95]

奥巴马的演讲水平很高，听他的演讲是一件让人感到舒服的事情。他在慷慨陈词之时，他的人气也在不断攀升。奇怪的是，奥巴马的演讲词里没有出现这两个词：“伊拉克”和“小布什”。这可能是无意的疏漏，但更可能是有意为之。但是，他用了很大篇幅在讲“情报”，这种强调反映出情报在猎杀本·拉登过程中的极端重要性。

美国人在“9·11”事件之后就开始追踪本·拉登，可他如同人间蒸发一样消失了，只在某些时刻发布视频宣示他的存在和不依不饶。美国情报人员知道他不用手机，也不上网，但他的命令和消息必须要传递出去。要做到这一点，他只能依靠中间人，美国人把这种中间人称为“信使”，也就是我们所说的“通信员”或者“交通员”。他们费尽九牛二虎之力打探到本·拉登的信使有个化名，叫作“阿布·艾哈迈德·阿库威蒂”（Abu Ahmed al-Kuwaiti）。可接下来锁定这个神秘信使花费了美国人四年时间。2010年8月的一天，在浩如烟海的电话监听记录中情报人员捕捉到了下面这段对话：

甲：你到哪里去了？我们很想念你。你过得怎么样？你现在都在干些什么？

乙：我回到曾和我在一起的那个人身边了。[93]

乍看起来，这不过是两个多日不见的老朋友之间非常普通的一段对话。当然，乙的话略有一点儿神秘兮兮，但也就仅此而已。可是，中情局的分析人员硬是根据这段对话分析出了这个乙就是本·拉登的信使。这就是奥巴马演讲中提到的“去年8月”获得的那条线索。

为了抓住本·拉登，中情局组织了上百名分析人员开展工作。分析人员的领导——为保密起见，记者管他叫“约翰”——十年如一日地追踪本·拉登，真是有一种“钉子”精神。为了找到本·拉登，他甚至拒绝了升迁的机会。在这一天，他的一个女下属起草了一份备忘录，题目是“逼近本·拉登的信使”。《华盛顿邮报》后来甚至在他们的网站上开辟了一个专栏，详细介绍本·拉登在阿伯塔巴德的住所、猎杀行动以及最后的海葬等情况，专栏题目就叫“逼近本·拉登”。[96]该专栏是向这篇备忘录致敬还是巧合，就不得而知了。又经过一个月的深度挖掘，备忘录终于完成。[97]

顺着信使的线索，美国情报人员找到了距离伊斯兰堡不到60公里的阿伯塔巴德镇。这个结果与很多人原来的预想大相径庭，但约翰对此并不意外，他知道“基地”组织的一些大头目就是藏身于闹市。[97]找到那座神秘的大宅并没有费太大力气，因为它过于神秘、太过不一般：整个院落占地大约1英亩（超过4000平方米），院子里有一栋三层小楼，占地面积大约是周围房屋的8倍。院墙高耸，墙头布满铁丝网，里面的住户从来不往外扔垃圾，只是每隔一段时间到院子的空地上把垃圾烧掉。[98]

绝大多数美国人一直认为本·拉登之所以能逃过追踪，是因为他或者躲在深山老林、荒野沙漠，或者藏匿于黑黢黢的地洞，整天不见天日，就像萨达姆一样。注意，这里说的是“绝大多数”，加州大学洛杉矶分校的两位地理学专家可不这么想。他们并非瞎猜，他们依靠的是科学。早在2009年，他们就计算出本·拉登不会那样做。他们正应了时下流行的一句话：“不能计算出本·拉登藏身之所的地理学家就不是一个好的情报分析人员！”

这两个聪明人一个叫托马斯·吉莱斯皮（Thomas Gillespie）、另一个叫约翰·阿格纽（John Agnew）。他们带领一群学生，独辟蹊径地运用物种分布的两种理论来计算本·拉登的藏身之地。第一种理论叫作“距

离衰减理论”，这种理论认为物种之间的相似性和相关性会随着距离的增大而减小。他们使用的另一种理论叫“岛屿生物地理学”，该理论认为规模较大、分布较为稠密的生命岛，比那些相对较小、彼此隔离的生命岛，能够支持更多的物种生存，并且让它们不易灭绝。

依据这两种理论，他们认为，如果本·拉登果真离开了他最后一个已知的藏身地点托拉波拉，他也不可能走得太远，并且本·拉登很可能躲藏在一个大城镇里，即使在这些大城镇被发现的风险要高一些，但是在那里可以得到更好的掩护。更重要的是，某些生存所必需的资源只有在这里才有可能得到。本·拉登每隔一段时间就需要进行一次肾透析，这是人尽皆知的，他距离医疗中心不能太远。这一结论和约翰的判断非常相似！专家们给出了非常明确的答案：本·拉登最可能藏身于巴基斯坦的帕拉奇纳尔。他们对本·拉登的住房情况也进行了推测，然后依据卫星地图锁定了这个城镇里的三栋建筑物。[99]事后来看，这个结论并不准确。的确，以托拉波拉为圆心，画出几个同心圆，其成为本·拉登藏身地的概率逐次递减，这样的模型过于简单和粗糙。

加拿大瑞尔森大学的穆塔扎·黑德（Murtaza Haider）教授对吉莱斯皮等人的研究进行了批评，他认为他们在分析过程中忽略了几个关键要素，最明显的就是没有考虑政治和历史背景。黑德教授本人来自巴基斯坦，他认为，只要了解历史知识，就能知道什叶派穆斯林和逊尼派穆斯林之间存在不可调和的矛盾，本·拉登不大可能躲在巴基斯坦部族地区中唯一一个什叶派穆斯林占多数的城镇，因为“基地”组织是一个极端的逊尼派穆斯林组织。[100]事后，吉莱斯皮教授也承认，他对自己这篇文章的结论也不太相信。并且尽管他对本·拉登藏身阿伯塔巴德镇的概率（88.9%）也做过估计，但他并没有在文章里明确地写出来。[101]

为了确定本·拉登的藏匿地点，美国人加紧了对这个重点院落的侦察。他们发现：院里的人接听电话甚至更换手机电池，都要跑到一个半小时车程以外的地方。美国人动用了他们掌握的各种先进技术——卫星和无人飞机。照片很快就送来了。情报分析人员仔细查看这些照片，有了一个新的发现：大宅里有一个男人几乎每天都会到庭院里散步，每次散步一两个小时。他们甚至给他起了一个外号叫“溜达”。估计这个“溜达”从不仰起脸庞，因为照片上从来没有出现过他的面部图像。美国人又想到了利用身高确定他是不是本·拉登，并且还估计出了一个身高的范围：5.8~6.8英尺（约1.77~2.07米）。[93]可惜这个范围过于宽泛，对

确定“溜达”是不是本·拉登意义不大——本·拉登的实际身高在6.4英尺左右（约1.95米）。为了得到更多情报，中情局在院子周围悄悄安排了特工进行近距离侦察。综合方方面面的情报，很多分析人员认为本·拉登在这个神秘大宅里的可能性达到六成，约翰比较乐观，他认为有八成的把握。[97]

在约翰的上司中，有三个迈克尔。第一个迈克尔是国防部负责情报工作的次长迈克尔·威克斯（Michael Vickers），他支持约翰的看法。[102]第二个迈克尔是美国国家反恐中心（NCTC）主任迈克尔·雷特（Michael Leiter），他比较保守，认定把握只有四成[93]，是约翰以及猎杀行动的主要反对者，也因此被赠予“四成先生”的雅号。第三个迈克尔是中情局常务副局长迈克尔·莫雷尔（Michael Morell），他意见居中，认为有六成的把握。[102]

最后的决定权在奥巴马手里。综合考虑各种有利和不利因素之后，他决定赌一把、放手一搏，最终批准了猎杀任务。[93]所以，当面对实时传回来的行动画面时，奥巴马的神情显得异常严肃，甚至可以说是非常紧张。

外国人也喜欢揭秘，他们自然不会放过大英雄约翰。经过一番深度搜索，关于约翰到底是谁，似乎有了一个答案，他的名字叫“斯蒂芬·尼括斯基”（Stephen John Nicgorski）[103, 104]，“约翰”是他的中间名。美联社说他就出现在那张著名的奥巴马猎杀本·拉登的照片里，并让大家特别注意照片中右侧那个系米色斑点领带、着深色西装的身影。[97]其实，除了这张“著名”的照片，在猎杀本·拉登行动前后，御用摄影师苏扎还从另外一个角度拍了一张“非著名”的照片。有兴趣的读者可以到Flickr网站上去找找这张编号为“P050111PS-0210”的照片[105]，背对着我们的是奥巴马，在他的前方、11点钟方向的最远端，有一个身材高大的男子，他就是约翰。

我们一般会认为战情室很小很拥挤，然而等看到这张“非著名”的照片才发现：这个房间的面积并不算小，站在远处的约翰显得非常模糊。

2012年圣诞季，一部名为“猎杀本·拉登”（*Zero Dark Thirty*）的好莱坞大片登上银幕，影片风格犀利，导演是执导过奥斯卡最佳电影《拆弹部队》（*Hurt Locker*）的凯瑟琳·毕格罗（Kathryn Bigelow），她成功地把纪录片那种真实感和力量感赋予了这部故事片，从而赢得了美国国

内媒体的一片好评。女主角玛雅是中情局女特工，“9·11”事件之后她就被派到美国驻巴基斯坦使馆工作，唯一的任务就是找到本·拉登。靠着常人无法想象的坚忍，她最终锁定了本·拉登的行踪，帮助海豹突击队完成了猎杀任务。据编剧马克·波尔（Mark Boal）说，这部电影里的所有角色，包括玛雅，都有原型。很多人认为这个角色和《艰难一日》（*No Easy Day*）注里的珍是同一个人。[106]有这样的想法也很正常。就在电影上映三个月前，准确地说是2012年9月4日，《艰难一日》面世，其作者是海豹突击队前队员，他以亲历者的身份披露了猎杀本·拉登行动前前后后的许多细节，此书一经出版立刻引起轰动。从某种意义上说，《猎杀本·拉登》引起的观影热潮和这本书的先期出版也有一些关系。而大家把电影中的玛雅与书中的珍相对应，就是顺理成章的一件事情了。书里有这样几段内容，给人留下了深刻印象：

我对她很好奇，因为她可是抓捕本·拉登行动的主要分析师之一。

“老实说，”我问她，“那人是本·拉登的可能性有多大？”

“100%准确。”她傲然回应。

……

以前我们也听过号称“100%准确”的情报，但每次结果都让人失望。

“别随便说什么100%。”我说，“咱们的情报人员说100%的时候，往往只有10%的把握。说10%的时候，倒更可能是100%确定。”

……

“不，不，”珍说，“确实是100%。”[107]

这样一个电影中的英雄，在现实生活是一个棱角分明的人。有知情人说，她在巴基斯坦的工作其实很多年都没有进展，几乎到了失败的边缘。直到奥巴马执政后，中情局的工作人员重新审查了若干条线索，猎杀任务才终于看到了一线希望。有一条线索表明本·拉登可能使用信使传递消息——她是最早相信并围绕这一线索开展工作的人员之一。后来，事实证明这条线索是对的，很多人都跑来争功，这让她很是恼火。在她获得杰出情报勋章之后，她终于忍无可忍——她从心底瞧不起那些跟

着“喝汤”、获得次等奖励的其他同事。[108]据前中情局官员说，她给这些同事群发了一封电子邮件，里面写道：

曾经试图给我设置障碍的就是你们这些人。你们都反对过我。只有我应该得到这份奖励。[108]

可以想象，发出这样一封邮件的人会有什么样的“群众关系”。总之，尽管她立了功、得到了一笔奖金，却没能获得职位晋升，而是被调去执行另外一项反恐任务。[108]由此可以得到一点启示：即使在美国，也必须注意处理好“群众关系”。

和约翰的情况不同，既没有人把她的真实姓名曝光出来，也没有人把她和约翰的关系交代出来。不妨大胆推测一下，她应该是约翰的手下，起草那份“逼近本·拉登的信使”备忘录的就是她。当约翰在白宫战情室陪着总统观看枪战实况转播的时候，她只能在美军的巴基斯坦基地里焦急地等待行动结果。

关于《猎杀本·拉登》这部电影，还有一点值得一提。这是一部典型的美国主旋律电影。在电影拍摄过程中，摄制组得到了美国军方的大力帮助。2011年7月，导演凯瑟琳·毕格罗和编剧马克·波尔想拜访一下美国国防部主抓情报工作的次长迈克尔·威克斯。刚开始，毕格罗他们以为最多有15分钟的谈话时间，没想到副部长居然给了他们45分钟，官方对这部电影的重视程度由此可见一斑。毕格罗他们大喜过望，因为这意味着他们有可能从军方高层那里获得大量一手信息，结果也的确如此。[102]

故事到这里，似乎该说的都说完了，但其实还有一个问题。很多人被轰轰烈烈的军事行动、眼花缭乱的英雄故事吸引，很容易忽略这样一个问题。如果回过头来把所谓的反恐战争的脉络重新整理一遍，会发现明显还有另外一条平行的线索：如果说抓获萨达姆依靠的是社交网络分析这种情报方法，那么猎杀本·拉登呢？

本·拉登的住处是怎样被发现的呢？通过信使。信使又是怎样被确定的呢？通过电话监听！曾有人说，击毙本·拉登的头功应归于约翰[109]，看来这种说法并不准确。头功应该算在由小布什发动的、高度秘密的监视行动上，而这次行动有一个代号，叫作“星风”。

---

1. 《艰难一日》中文版已由中信出版社于2012年出版。——编者注

第二回 “星风”在行动

白宫。

“9·11”事件后大约半个月。

国安局局长海顿跟在中央情报总监特内特身后，走进总统办公室。这是他第一次到这里开会。一进房间，海顿发现总统本人、副总统切尼、国家安全事务助理以及总统幕僚长都已经坐在里面了。不久前，海顿曾经和中央情报总监以及副总统的手下讨论过，如何加强和改进情报搜集工作。他对总监说：“我们似乎永远都处于一种‘再打一个坏球就要出局’的状态。”特内特安慰他说：“我明白。”[13]

今天，他们要向小布什汇报一件大事，请他定夺。海顿画了一张图，上面画了三个圆圈，第一个表示希望得到的情报，第二个表示可以得到的情报，第三个则表示可以合法得到的情报。国安局能做的是，处理这三个圆圈的交集部分。切尼说，别管第三个圆圈，因为要讨论问题，就得先忘记法律。[110]

在这次会议之前，总监已经见过总统，把海顿他们在“9·11”事件之后考虑要做的事情做了汇报。小布什也很清楚海顿所说的“再打一个坏球”是什么意思，他告诉国安局局长：“我很理解你担心的问题，我们必须要做些事情来解决这些问题。我认为我有这个权力，可以授权你去做你们提出来的那些事情。”[13]话虽这么说，可小布什心里很清楚，他的这套说辞、他们在这间办公室里密谋要做的那些事情，迟早有一天会被曝光并且注定将引发争议。[17]但他决心已定，对海顿说：“你回去制订一个计划，然后拿来给我，剩下的事就让律师去处理吧。”[111]

局长内心久久不能平静。律师告诉他，总统的确可以授权，但历史上还从来没有哪个总统这样做过。晚上回到家中，他跟夫人商量着，想出去散散步。两人绕着米德堡总部边走边聊。总部周边丛林茂密，非常适合散步。夫人问他：“你是有什么心事吧？”由于事涉机密、无法细述，海顿只能这样含含糊糊地回答：“我们要做一件事情。总有一天，它会大白于天下。等到那时，它会引起很大的争议，所有参与这件事情的人都会被卷进去。”[13]

“传家宝”

1945年8月，纽约。

“二战”的硝烟终于散去，另一场没有硝烟的战争却一直没有平息。

美国陆军信号安全局（SSA）的工作人员依然忙忙碌碌，他们这段时间的主要工作是跟通信商接洽，希望获得他们的支持，监听进出美国以及过境美国的外国政府的电报通信内容。国际电话电报公司（ITT，简称“国电公司”）明确表态，拒绝参加这一违法行动。西联电报公司（WU，简称“西联公司”）则表示，只要有司法部部长的签字，他们就可以参加行动。在成功说服西联公司之后，信号安全局转过头来继续约谈并胁迫国电公司，面对压力，公司只得同意，但也提出和西联公司相同的要求：看到司法部部长的签字后再配合行动。接下来，信号安全局用相同的办法“做通”了美国无线电公司（RCA，简称“美电公司”）的工作。[112]

秘密行动在悄悄推进。接下来要解决的是具体的技术问题：怎样监视？把有关的电报通信数据全都交给信号安全局，这当然是最安全可靠的监视方法，但这样做需要的数据量太大。美电公司的通信流量经理威廉·斯巴科斯（William Sparks）想出了一个主意：把这些电报的发送者和接收者等关键数据（也就是我们现在常说的“元数据”）交给军方就足够了。斯巴科斯是美军陆军信号部队的预备役中校，对有关的技术情况非常了解。但他的这种想法很快就被军方否定了：所有有关的电报数据或者数据拷贝都要交到信号安全局手里。[112]

“二战”结束后，美军进行了大规模的体制和机制改革。最重要的几件事包括：成立国家军事部（NME），在陆军航空兵的基础上成立空军部，1949年，美国国家军事部改称国防部（DOD）。陆军信号安全局先是改名为陆军安全局（ASA），而后各军种信号情报部门合并，成立武装力量安全局（AFSA），为国防部下属机构。1952年，武装力量安全局改名为国家安全局并沿用至今。[112]所以，这里的一个基本“常识”是：美国的国安局隶属于国防部。

尽管情报组织的架构不停地变迁，这项原本为监视外国政府的军事

行动却一天也没耽误，多年来一棒一棒地接力下来，传到了国安局手里，并有了一个行动代号，叫作“三叶草”。国安局一直充当着美国国内情报单位的信息中介角色，他们将搜集到的信号情报信息分发给中情局、联调局等机构，这些机构都在国安局里设置了长期的联络办公室。[112]

随着时光流逝，“三叶草”行动也在悄悄发生变化。行动对象最初被严格限定为外国政府和机构，后来逐步扩展到所谓的“可能受到外国影响”的激进分子。[112]所有这一切都按部就班，并且进行得神不知鬼不觉，上面也再没有人关注这个行动了，国安局也再不需要向上面请示汇报。据长期担任国安局常务副局长的路易斯·托德拉（Louis Tordella）回忆，他只在1973年向国防部部长汇报过这个行动的情况，这是十多年中唯一的一次汇报。[113]

20世纪50年代，“三叶草”行动使用的是穿孔纸带。[113]每天，通信公司都会收发许多电报，并且都要借助这种纸带。发报人写好文字，通信公司将其转译为穿孔指令，在纸带上按照一定的编码方式打上小孔，再用机器发送出去。机器接收到来电，先是自动在纸带上打孔，再由读报员或者机器将其转译成文字，誊写或者打印到专门的电报纸上。其实，现在的eBay（易贝）上就有很多这样的古老电报纸在出售。对通信公司来说，这些穿孔纸带用过后就成了没有用处的废物。所以，这一时期国安局每天派专人把这些一卷一卷的穿孔纸带运回总部，还可以算是一种废品回收。纸带到了国安局，则开始了它的另一轮用途，情报人员可以全面解读上面的信息。如果你有机会查一下穿孔纸带的资料，看看几十年前这些简单而优雅的设计，很可能会从内心深处涌出一种感慨：抽象的信息就这样变成了具象的编码，原来现代信息组织技术发展史的开端就在这里！

到了60年代，磁带开始大量投入使用。同穿孔纸带相比，磁带的体积大幅缩小，并且可以重复使用，通信公司决定保留这些电报磁带，之前的穿孔纸带他们则没有留下备份。所以，国安局必须找个地方来进行磁带拷贝工作。他们找到了中情局，以中情局的名义在纽约租用了一个地方复制磁带。1973年，中情局退出，国安局只好另想办法，他们在曼哈顿区租用了一个地方继续开展磁带复制工作。每天，都有一个信使从国安局总部出发，乘坐火车来到纽约，把复制好的前一天的电报磁带装好，再乘车回到国安局总部。风雨无阻，每天如此。[113]外国机构发

送的电报多半是经过加密的，而加密和解密历来就是国安局的强项，他们会想尽各种办法把这些电报都解密出来。前面提到的托德拉就是一位密码专家，从本科到博士研究生阶段一直都在数学专业学习，早年还参加过破解德军“恩尼格码”密码机的工作。这项破译工作不仅为盟军获得“二战”最后的胜利立下了汗马功劳，并且对日后密码学、信息学、计算机科学等学科的发展都具有里程碑意义。

可以说，美国是在越南战争的枪炮声中进入60年代的。随着美军在战争中越陷越深，美国人对这场战争的态度逐渐明确，反战的声音也越来越强烈。1967年秋，发生了名为“向五角大楼进军”的大规模抗议活动。美国陆军整理了一份抗议者名单，要求国安局对这些人进行监视。接下来，中情局、联调局以及国防情报局都交给国安局一份类似的名单，名单上有民谣歌手琼·贝兹（Joan　Baez）、儿科专家本杰明·斯波克（Benjamin Spock）、女演员简·方达（Jane Fonda），还有著名民权运动领袖马丁·路德·金（Martin　Luther　King, Jr.）。黑名单越来越长、名单上的人越来越多，甚至与名单上的监视对象有任何关系的人都会受到株连。[114, 115]

国安局的这项行动在1969年7月1日被正式批准，代号“光塔”。[114]行动批文上写道：

“光塔”信息特指参与民众骚乱、反战示威和活动的个人或组织，以及参与反战活动的军事人员的通信信息……尽管“光塔”是信号情报行动，有关材料将分发给信号情报用户，但在这些材料上不要标识“国家安全局”的字样。[114]

也就是说，国安局不仅要执行好“光塔”任务，还要把自己参与过的种种非法监视活动的痕迹彻底抹掉。联调局局长埃德加·胡佛（Edgar　Hoover）突发奇想，认为美国的“贵格派”组织向东南亚运送食物及其他物品，他要求国安局对所有的贵格派教徒进行监视。胡佛局长显然忘了，尼克松总统自己就是贵格派教徒。[114]不知道最后国安局有没有因此对尼克松进行监视，但尼克松确实一直疑心自己被国安局监视。[114]1973年，由于司法部部长艾略特·理查森（Elliot　Richardson）质疑“光塔”行动的合法性，这一行动随即终止，而此时被列入黑名单的已有600多人。[113]

从1967年起，中情局启动了一个秘密监视行动，代号“混沌”。行动

最初是响应白宫的要求，调查美国本土反战抗议活动背后的海外黑手，但让白宫失望的是，调查的最终结果是，根本没有什么海外黑手。于是，“混沌”行动的枪口转向了国内，把美国人作为主要监视对象。[116]中央情报总监理查德·赫尔姆斯（Richard　Helms）就接到过国家安全事务助理亨利·基辛格（Henry　Kissinger）的命令，要他提供反战罢市的各团体领导人的所有信息。[117]就这样，中情局在“混沌”行动中收集整理了7200个美国人的“黑材料”，在数据库里保存了大约30万美国人的数据记录，为联调局和其他政府部门提供了上千份相关报告。[116]中情局搞不清楚不同的反战团体之间在立场上的区别，于是把这些组织一股脑儿全列为监视对象。当然，监视计划要落地还得仰仗国安局强大的监听能力。[118]

尼克松手下有个年轻的律师，名叫汤姆·休斯敦（Tom　Huston），是个退役陆军情报军官，年仅30岁，也算是青年才俊吧。1970年6月，尼克松召集国安局、中情局、联调局和国防情报局的负责人开会，休斯敦也列席了这次会议。会上，总统说：

根据白宫得到的情报，我确信，情报界在搜集与激进组织活动有关的情报工作方面，没有投入足够的人力物力。[114]

会后，休斯敦很快就起草好了一份备忘录，7月，尼克松签字批准了这份绝密文件。[119]该文件授权国安局“制订计划，利用其国际设施对美国公民的通信情况开展监视行动”。不需要调查令，也不需要任何理由，每个人的国际电话和国际电报都可以被监听和被散发，再无隐私可言。这份文件后来被称作“休斯敦计划”。[114]文件也解除了对情报机构的其他一些限制，比如可以破门而入拿到他们想要的材料。休斯敦在文件中写道：

这等于是入室盗窃，因而具有很高风险，一旦曝光，将会带来巨大的尴尬。[120]

联调局局长胡佛读到文件后“怒气冲天”，因为文件上还有这样一段话：“联调局没有能力监听国际通信，而国安局正在有限的范围内开展这一工作，并且提供了非常有用的信息，其中很多信息对白宫特别有用。”这分明是在挑战联调局长期独霸的领域。胡佛直接冲进了司法部部长约翰·米切尔（John　Mitchell）的办公室，要求他收回成命。米切尔说，这份文件里所说的这些行动都是违法的，不可能是总统的决策。部

长马上去找尼克松，最终说服了他——在签署文件五天之后，尼克松又撤销了这份文件。[114]

国安局的心情像经历了一次过山车，先是对“休斯敦计划”得以迅速签署欣喜万分，然后又因为计划被匆匆取消而十分恼火。多年来，他们一直在没有得到授权的情况下收集国内情报，不能因为这次总统收回成命就罢手。事实上，越来越多的美国人被国安局拉入了黑名单。[114, 115]

不久，休斯敦接到通知，他手头的工作转由约翰·迪安（John Dean）负责，这也是一位年轻的律师，先前在司法部部长米切尔手下工作，此时是尼克松的法律顾问。他拿到“休斯敦计划”后，直接把文件扔进了自己的保险箱。[114, 115]

1971年6月中旬，尼克松把基辛格和白宫幕僚长“鲍勃”·霍尔德曼（“Bob” Haldeman）找来，商量一件事情。霍尔德曼猛然想起，布鲁金斯学会有一份材料，非常符合总统的需要。但尼克松深知这个机构与民主党关系密切，甚至被叫作“民主党国家委员会”，想要他们把材料交出来无异于与虎谋皮。

尼克松说：

鲍勃，你还记得“休斯敦计划”吗？去执行它吧……我的意思是，去偷。该死的，直接闯进去，把材料拿到手。炸掉保险箱！拿到东西！[121]

过了半个月，尼克松再次指示霍尔德曼和基辛格：“破门而入，搞到文件，明白吗？”第二天一早，他又说：“鲍勃，赶紧把布鲁金斯学会那件事办了，我要得到那个被炸开的保险箱。”那天晚些时候，他再次催问：“你安排谁去布鲁金斯学会了？”不知何故，这次“破门而入”计划最终并未实施。[122]尼克松显然忘记了，他已经在一年前亲自取消了“休斯敦计划”。

“水门事件”爆发。最让尼克松受伤的是迪安的背叛。1973年6月，为了争取免于被起诉的机会，迪安把“休斯敦计划”作为交换条件交给了检方，[115]不仅如此，他还在听证会上指控尼克松积极参与掩盖丑闻的种种活动，并且授意给被捕人员“封口费”，让他们保持缄默。迪安讲了这样一件事：一天，尼克松问他，除了已经花掉的46万美元，让他们

继续保持沉默还需要多少钱？迪安想了想，告诉总统说，大概还要100万美元。尼克松当即表示，钱不是问题。[123]

此外，迪安还供出了参与事件的核心人物霍尔德曼和约翰·埃利希曼（John Ehrlichman），他们俩参加了总统组织的许多次商议掩盖丑闻的专门会议。1973年1月之前，迪安通常向他们汇报自己承担的掩盖任务的进展，1月之后，尼克松开始直接找迪安，询问掩盖行动的情况。[123]

1974年8月8日，尼克松在各方压力之下终于辞职，大家都以为“水门事件”到此结束，终于可以消停了。然而，4个月后，又发生了一件大事。《纽约时报》记者西摩·赫许（Seymour Hersh）争取到了一个采访中央情报总监威廉·科尔比（William Colby）的机会。科尔比向记者透露了许多情况，他试图说服赫许，所谓“非法监视”都是些不值一提的小事情，家丑不宜外扬。赫许马上意识到自己钓到了一条“大鱼”，他连夜赶写出稿件。[124]第二天，也就是12月21日一早，一篇揭露中情局黑幕的重磅文章就刊登在了《纽约时报》上，头版头条，通栏的大字标题是“尼克松时代，中情局针对美国反战力量和持不同政见者展开了大规模行动”，标题下面是尼克松时代三任中央情报总监的大幅照片，他们是赫尔姆斯、詹姆斯·施莱辛格（James Schlesinger）和科尔比，以告诉读者这三个人对大规模非法行动负有首要责任。

文章开头就写道：

据来自政府的消息灵通人士称，尼克松执政期间，中情局直接破坏了对它进行约束的章程，非法地、对美国国内的反战运动和其他持不同政见团体采取了大规模的情报搜集行动。

本报经过广泛调查证实，中情局的某个特别部门保存着至少一万名美国公民的情报材料，这个部门直接向当时的中央情报总监赫尔姆斯报告工作……

消息人士还透露，赫尔姆斯先生的继任者施莱辛格去年下令对中情局掌握的国内材料进行检查，结果发现，从20世纪50年代开始，中情局在美国境内采取了数十次非法行动，包括非法闯入、窃听电话和私拆信件等。[125, 126]

看到这样一篇文章，科尔比想必后悔不迭。他想起了另一件更为紧

要的事情。一年前，他的前任施莱辛格起草了一份备忘录，发给中情局的每个人：

我已命本局所有高层官员，立即向我报告正在进行之中或已事过境迁但可能构成违反本局章程的一切行动。

本人在此指示，目前受聘于本局的所有同人，将所知的上述活动直接向我报告。同时，也请已离职的职员比照办理……[127]

中情局的章程内容极为含糊，但有一点相当明确：中情局不得成为美国的秘密警察。然而实际情况是：多年以来，中情局一直在监视美国公民，窃听他们的电话，拆阅他们的信件。一周之后，一份700页的材料被整理了出来。而此时，施莱辛格却已经奉命调到国防部——他在中央情报总监的位置上前后只待了17周。[127]这份绝密材料顺理成章转到了新任总监科尔比手里，资料封面上醒目地写着“传家宝”这几个字[128]——科尔比当然知道，那里面的内容一点儿美好的意味都没有。这份资料里记录的是1959年以来中情局所做的种种丑恶勾当，例如针对国内新闻记者的“知更鸟”行动、“丁烷”行动、“纤维板一号”和“纤维板二号”行动，还有为确定某人是否掌握未经授权的涉密信息的“红脸一号”行动等，当然还有许多更为不堪的事情。这些信息一旦泄露，中情局有可能无法继续存在下去。[124, 128]

事不宜迟，科尔比赶紧准备好了一份加长电报传给基辛格，概要地把“传家宝”的情况汇报了一遍。基辛格立即把这份长电报的内容浓缩为五页纸的一份备忘录，在圣诞节这一天交给了杰拉尔德·福特（Gerald Rudolph Ford, Jr.）总统。[124]尽管随后国会花了一整年时间调查这份备忘录涉及的各种事情，“传家宝”里的秘密也陆陆续续被曝光出来，但中情局直到2007年才正式完整解密了这份绝密资料。[129]

情报单位的“为非作歹”与国会监督流于形式不无关系。1973年，中央情报总监施莱辛格告诉参议院武装力量委员会主席约翰·斯坦尼斯（John Stennis）说，他希望汇报一下某项即将开展的行动。斯坦尼斯连声回答：“哦，不，不用。不用向我汇报，你们做就行了！我不想知道这些事情。”[130]

美国主流媒体对情报单位丑闻的密集报道最终引起了国会的关注。1975年1月底，参议院正式成立了“政府情报活动特别调查委员会”，由

参议员弗兰克·丘奇（Frank Church）担任主席，这就是后来对美国情报工作产生重大影响的“丘奇委员会”。[125]

“现场报告”

丘奇委员会跟之前的情报活动调查委员会极为不同，它下面设立了若干个调查小组，专门调查情报单位非法的、不正当的、不道德的行动，而从前那些委员会主要想解决情报单位的组织问题、管理问题和效率问题。丘奇委员会从副总统尼尔森·洛克菲勒（Nelson Rockefeller）那里拿到了“传家宝”文件的一个副本，从中立刻得到了很多调查中情局的具体线索，再加上中情局和联调局都曾经多次被新闻媒体曝光，顺着“传家宝”的线索和有关的新闻报道追查下去，丘奇委员会对这两家单位的调查工作进展顺利。[113]

剩下的一个重点调查对象是国安局，因为它之前几乎从未在媒体上出现过，人们对它的印象是一个面目模糊的神秘“巨人”，还根据它的首字母缩写“NSA”送给它一个“查无此局”（No Such Agency）的外号。这项艰巨的任务交给了调查小组里的年轻人，让他们去闯一闯、试一试。后来成为中情局总监察官的布里特·斯奈德（Britt Snider），和另外一个伙伴一起，承担了对国安局的调查工作。那一年他正好30岁。可别小看这个斯奈德，他刚刚通过了一次调查“大考”，积累了不少经验。前面曾提到，美国陆军在越战期间通过国安局对美国公民展开情报监视，除此之外，他们还自己动手进行监视行动。这件事被曝光后，斯奈德就参加了对美国陆军情报单位的调查工作。

克里斯托夫·派尔（Christopher Pyle）现在是蒙特霍里约克学院的政治学教授，1967～1968年他担任过陆军情报学校的老师，有上尉军衔。他需要在一堂课上讲授陆军在美国本土的情报和现场报告工作。所谓现场报告，是指针对某一事件撰写出来的报告，形式上通常分为六段。由于不了解实际情况，他只能凭着自己的想象去拼凑这堂课的内容。以其昏昏，岂能使人昭昭？有位年轻的军官实在听不下去了，就邀请派尔老师去实地参观一下，增加一些感性认识。等到了他们工作的地方，派尔大吃一惊。[18, 131]

那里曾经是一个机车车间，外墙黑漆漆的、车间的空间巨大，派尔拿到一些“书”，可这哪里是什么书啊，封面上是一些大头照。他一眼就认出了一张熟悉的面孔——拉尔夫·阿伯内西（Ralph Abernathy），派

尔记得他是马丁·路德·金的助手。“书”的旁边堆着穿孔卡片，这在当时算是最先进的信息技术产品了。他们告诉派尔，原始的信息由大约1500名陆军特工搜集汇总，在这个大房间里摆放着十几台电传打字机，专门用来接收特工们上传的现场报告。这些特工由美国各地大约300个办公室管理，他们原来的主要任务是安全身份审查，这段时间则增加了一项新的职责：监视国内各种持不同政见的人员。很快，派尔又看到了另一个熟悉的名字——阿尔罗·塔图姆（Arlo Tatum），他是“费城拒服兵役的有良知人士委员会”的负责人，这是一个反战组织，派尔曾经和塔图姆有过一点儿联系。[18, 131]此刻，派尔老师可能觉得后背发凉——自己是不是也被监视了？

在派尔的请求下，他们交给他1968年3月11～18日这一周时间内收到的现场报告，作为他课堂使用的实例。其中一份报告说的是特工参加某次“独神派”教会活动的情况。派尔想，连教堂也逃不过被监视的命运，这个国家怎么了？这个国家还会怎么样？实在应该做些事情来改变这一切。[18]不久之后，他如期退出现役，把自己的“发现”告诉更多人就成为他的头等大事。1969年冬天的一个早晨，派尔走进了参议院，把他看到的、知道的一切都告诉了那里的工作人员。[46]并且，他很快还完成了一篇报告，发表在1970年第一期的《华盛顿月刊》上。[132]

派尔告诉大家，陆军情报司令部正在监视普通美国人的各种活动，秘密搜集他们的材料，并且利用其覆盖全国的电传网络，把情报集中到它的中心计算机数据库里。他的恐惧源自美国人对不受约束的权力持怀疑态度的传统。他还说，国会和法院都没有对陆军情报系统进行过足够的监督。[132]派尔的这篇文章引起了巨大轰动，也戳到了国会的痛处。这其中有一位“老黄忠”似的人物，参议员萨姆·埃尔文（Sam Ervin），这一年他已年过70。埃尔文和十几个议员一起，要求军方立即给个说法。面对质疑，陆军的第一反应就是掩盖，他们显然低估了埃尔文的决心和毅力。调查委员会已经成立，熟悉情况的派尔被埃尔文聘为委员会的调查顾问，他在6月又写了一篇文章，专门揭露军方的种种掩盖手段。在这个节骨眼上，埃尔文收到一封信，寄信人名叫约翰·奥布瑞恩（John O’Brien），他曾经是陆军情报中士，在德国服役三年后他回到伊利诺伊州，参与了美军在国内的监视行动。他向埃尔文反映，这些监视行动毫无节制，甚至连伊利诺伊州的参议员阿德莱·斯蒂文森（Adlai Stevenson）、众议员阿伯纳·米克瓦（Abner Mikva）以及前州长奥托·科内尔（Otto Kerner, Jr.）等头面人物都在他们的黑名单上。

[133, 134]国会这回真的被激怒了。

很快，埃尔文就主持召开了一系列公开听证会，题目只有一个——“联邦数据库、计算机和权利法案”，效果极为轰动。派尔事后回忆：“满屋子都是记者，人多到要卖‘挂票’。”[134]这些听证会为埃尔文赢得了普遍的尊敬，也使得他日后成为“水门事件”调查委员会主席的不二人选，在他个人的历史上留下了浓墨重彩的一笔。原来人真的可以像黄忠那样，在70岁以后迎来人生顶点！

尽管埃尔文的听证会没有揭露出陆军秘密情报行动的所有细节，但严重动摇了军方要死扛到底的信心——陆军最终彻底终止了他们的行动，并且彻底销毁了他们收集整理的所有情报。[131]因为他们担心，万一将来有人根据《信息自由法》要求披露这些见不得光的“黑材料”，结果肯定会更麻烦。[46]不仅如此，原本由一个少将领导的陆军情报司令部（AINTC）也降格为陆军情报局（AINTA），改由一个上校领导，几年后并入陆军情报与安全司令部（INSCOM）。[135]

这次事件也成为派尔自己的人生拐点。1970年秋，正在撰写博士论文的他突然找不到感觉了，原先确定的题目似乎永远也写不到头，于是他果断地把已经写了大半的论文扔进了垃圾桶，转而以陆军监视行动为主题重起炉灶，顺利拿到了哥伦比亚大学博士学位。[131]

揭秘“三叶草”

施奈德从1971年开始就参与调查美国陆军情报机构，一直到1974年整个调查工作结束他才离开，在此过程中增长了才干，也积累了经验。这次接到调查国安局的任务后，他和同伴马上跟国会研究部（CRS）联系，请他们把所有提到国安局的公开资料整理成一份材料。研究部很快就交差了——总共只找到两份资料，一份是《美国政府机构手册》上的一段描述，另一份是《滚石》杂志上一段错误百出的文字。[113]看来“查无此局”真的不是浪得虚名！

施奈德想到了国安局的“财神”——参议院武装力量委员会和拨款委员会，这两个委员会负责国安局的年度经费问题，可每个委员会里只有一个工作人员稍微了解一点儿国安局的情况，并且也只是知道预算和项目经费情况，至于国安局的具体运作情况，无人关注，也无人知晓。施奈德还走访了国安局的一些退休职员，从他们口中了解到的最严重的权力滥用问题竟然只是停车位分配这样的鸡毛蒜皮的小事。[113]

1975年5月，施奈德及其同事拿到了中情局的“传家宝”，仔细阅读之后，他们终于从中发现了两条与国安局有关的线索。其中一条线索最终导致了一个惊天秘密的曝光。这到底是怎样的一条线索呢？在解密后的“传家宝”文件里，有这样一段话：

使用中情局的经费和运作机制，□□□□为联调局购置了一处房产，用来放置国安局的技术设备，该处房产专门用于□□□□□□□□□□□□。[128]（□是文件解密时被删掉的字句。）

施奈德多年后在文章中回忆，他们找到的一条线索揭露出中情局在纽约为国安局准备了一处办公场所，专门用于复制电报。[113]很可能就是上面这段话了！

施奈德马上要求国安局汇报有关事项。国安局也很快给出了答复：由于此事高度敏感，只能向调查委员会主席丘奇和副主席约翰·托尔（John　Tower）单独汇报。[113]施奈德心知肚明：对方这是在故意设置障碍，丘奇是民主党人，托尔则来自共和党，在不少问题上两人意见不一，托尔甚至拒绝在委员会的最终报告上签字[130]。让他们同时出

现来听取国安局的汇报，基本上没有可能。调查工作陷入了僵局。

8月初，《纽约时报》披露了国安局窃听美国公民国际通信的情况，顺便还提了一下进行之中的调查工作。这回国安局方面坐不住了，很快就安排好了专门的汇报会，向调查组解释有关情况。在这次会上，国安局终于首次承认了“三叶草”行动，并且告诉施奈德，这项行动已经在5月由国防部部长下令终止了。至于为什么终止这一行动，他们给出的理由是“行动没有产生太大的价值”。这显然是欲盖弥彰。行动是什么时候开始的、怎样开始的、谁批准的，面对调查组这些咄咄逼人的问题，汇报人的答案相同：不知道。不过汇报人还是给调查组提供了一条非常重要的线索：托德拉可能是唯一健在的知道所有情况的人。[113]

托德拉是国安局的元老和常青树。“二战”期间，他投笔从戎，离开大学校园进入海军OP-20-G密码部队，先后参与了破解德军和日军密码的工作。他1949年就进入了武装力量安全局，那时候这个机构刚刚成立，不久改名为国安局。托德拉凭着自己的优异表现和才干“进步”神速，1958年就当上了国安局副局长，那一年他47岁。托德拉很早就倡导在密码工作中运用计算机技术，他对计算机科学和密码工程的概念有着深刻的理解，是研发超级计算机的有力推动者，国安局后来决定以他的名字命名超级计算机大楼。由于他做出的突出贡献，当他1974年从副局长位置上退休的时候，托德拉被授予国家安全勋章、国家情报工作杰出勋章，这是美国情报界的最高奖项。他还有两个外号，“T博士”和“诺博士”（Dr.No）。[136, 137]熟悉“007系列”的人都知道，第一部邦德电影就叫“诺博士”，在这部电影里，诺博士是个大反派，但是，不知道为什么托德拉会得到这样一个外号。

施奈德很快就和刚退休不久的托德拉联系上了。在调查组面前，托德拉将自己掌握的“三叶草”行动的相关情况和盘托出。他告诉调查组，参与行动的这几家大公司完全是出于爱国心行事，政府要求他们干什么，他们就干什么，他们认为这些事情对国家安全非常重要，“他们没有从行动中得到过一分钱的好处”。他认为，这些公司确信哈里·杜鲁门（Harry Truman）总统和司法部部长汤姆·克拉克（Tom Clark）知道并且准许“三叶草”行动。当被问到国安局有没有利用“三叶草”行动监视美国公民的国际通信时，托德拉回答说：从原则上讲，国安局对此类信息不感兴趣，不过，国安局会根据一些美国公民的名字，把他们的国际通信信息筛选出来，这样的事情发生过若干次。尼克松执政期间，国安局

曾经考虑将这项任务转交给联调局，但联调局没有同意。尽管国安局里很多人都知道有这么一件事情，但前后只有两个人具体负责过此事，其中一个人从1952年一直干到1970年退休，另外一个人从1970年之后接着做，一直到最近。[113]

几天后，国安局正式向委员会汇报“三叶草”行动，印证了托德拉所说的情况基本属实。委员会要求国安局局长小卢·艾伦（Lew Allen, Jr.）参加有关“三叶草”行动的公开听证会，但遭到了当时福特政府的拒绝。在此情况下，委员会一致决定公布调查报告。这下福特总统沉不住气了，他给丘奇和委员会的其他人打电话，说有关内容涉密、不宜公开，请他们三思而后行。司法部部长爱德华·列维（Edward Levi）也向委员会施加压力。丘奇有点儿顶不住了，他让大家投票决定。多年以后，施奈德回忆说：

这是有史以来的第一次：国会的委员会投票推翻了总统的提议，决定把总统认为应予以保密的信息发布出来。[113]

1975年11月6日，丘奇在国会公布了对“三叶草”行动的调查报告：

“三叶草”是1945年8月至1975年5月国安局开展的一项特殊行动计划。其间，绝大部分从美国发出的国际电报内容都被交给了国安局。两家参与行动的国际电报公司（美电公司和国电公司）提供了几乎所有发到美国的国际电报内容。第三家参与行动的公司西联公司在1945～1972年仅提供了特定的国际电报内容。“三叶草”行动可能是历史上最大规模的政府监视计划。尽管无法知道整个行动总共获得了多少电报信息，但是据国安局估计，在行动最后的两三年时间里，每个月都能得到大约15万条电报内容。[138]

“三叶草”行动是丘奇委员会最为意外、最为震惊的一大“发现”，它揭开了国安局的盖子。委员会以“传家宝”文件为线索，顺藤摸瓜，把中情局查了一个底朝天。当然也不能放过联调局，它们的“反情报”行动等秘密计划也被曝光。委员会还对马丁·路德·金和肯尼迪总统遇刺案的调查情况进行了再调查。简而言之，这是美国历史上国会第一次针对情报机构进行如此系统、如此全面的调查行动。在15个月的时间里，丘奇委员会一共举行了21次公开听证、250次行政听证、126次全体会议、40次小组会议、前后约见了800多个人，最后公开发表了14卷听证记录和报告，并且向参议院提出了183项建议，可谓硕果累累。[125, 130]

众议院在参议院丘奇委员会成立后不久，也成立了一个调查委员会，可由于指派的委员会主席出现问题，他们的这个委员会很快夭折。众议院随后通过一项新的决议，另行成立一个调查委员会，由众议员奥蒂斯·派克（Otis Pike）担任主席，该委员会也被称为“派克委员会”。可由于种种原因，委员会未能公布其最终调查报告，产生的作用和影响十分有限。

对国安局和其他情报单位所拥有的技术能力，丘奇深感不安，他大声疾呼：

（国安局）有能力监视一切：无论是电话、电报，还是其他。他们的这种能力随时可能转向用于美国人民身上，一旦如此，美国人将毫无隐私、无处可藏……我们有责任确保这个单位，以及所有（情报）单位，在法律允许的范围内，在适当的监督之下运用这种技术能力，只有这样我们才永远不会跌进那个无底深渊。[139]

根据丘奇委员会的建议，1976年5月，参议院通过了SR400决议，建立“情报特别委员会”（简称“参议院情报委员会”）。一年后，众议院通过了HR658决议，建立“永久情报特别委员会”（简称“众议院情报委员会”）。从此，国会有了正式的、常设的情报监督机制。参众两院的这两个情报委员会既有“特别委员会”的特点，又有“常设委员会”的特点。[140]

“特别委员会”中的“特别”一词，对应的英语单词并非“专门的”（special），而是“精选的”（select），意思是说，委员会成员是由两院政党领袖挑选出来的。参议院情报委员会共有15个名额：其中两党分别从拨款、武装力量、外交、司法4个委员会中各推荐1人，这就用掉了8个名额；剩下7个名额，多数党推荐4人、少数党推荐3人。[141]除了这15个人，两党领袖、武装力量委员会主席和副主席是这个委员会的必然成员，但他们都没有投票权，也不被计入委员会的法定人数之内。当然，如果他们是前面提到的4个委员会成员则另当别论。[142]众议院情报委员会的名额和政党比例不定，从最初设定的16人，逐步增加到上一届的20人、这一届的21人，两党人数比例上一届是12：8，这一届是12：9。参议院情报委员会建立之初曾规定委员最长任期为8年，2007年修订SR400决议时，取消了这条限制。众议院情报委员会规定委员最长任期为6年。[56, 140]

作为“常设委员会”，两个情报委员会和国会其他常设委员会类似，拥有立法权，可以进行立法提案，并且拥有长期不变的职责范围和常设的委员会助手。这些特点有助于国会更好地履行监督职责。[140]参议院情报委员会有权监督美国政府所有从事情报活动的部门或单位的情报活动，还有权对中情局、联调局、国安局、国防部和国务院下属情报机构进行预算监督。众议院情报委员会的监督管辖权大体上也是这样。[125]

在上一回中曾提到，就伊拉克战争情报失误问题，2004年2月小布什以总统令的形式宣布成立一个独立调查委员会开展调查工作。其实，在他的这个委员会成立之前，准确地说是2003年6月，参议院情报委员会就已经正式启动了“伊拉克战争战前情报调查工作”。与白宫的调查委员会临时搭班子、找人“背黑锅”不同，参议院情报委员会开展调查工作属于本职要求，也更为客观公正。他们把调查工作分为两个阶段，第一阶段围绕情报生产问题，第二阶段围绕情报使用问题，后面这一问题是小布什的独立调查委员会极力回避的。但由于国会选举和党派的影响，以及行政机构的干扰等原因，这次调查前后历时5年，到2008年6月才全部结束。参议院情报委员会先后发布了6份调查报告，主要结论总结起来就是两句话：情报界战前提供的情报评估的确存在很多错误；但决策层罔顾情报界在战前发出的种种警告，执意发动战争，自身也难辞其咎。[56]

特密专案

丘奇委员会的成果，不仅促成了国会参众两院情报委员会的建立，还直接催生了《外国情报监视法案》。这部1978年颁布的法案可以被看作规范和限制美国总统以及情报部门监视权力的一个“笼子”，它的诞生是美国情报工作历史上具有里程碑意义的重大事件。

这部法案规定，像“三叶草”行动那样未经许可就大范围窃取美国人通信信息的行为是非法的，随意把美国人列入监视名单也是非法的。依据这部法案，专门设立了由11人组成的外国情报监视法庭（FISC）。国安局以及其他政府部门如果要监视某位美国公民，或者监视拥有永久居住权，也就是俗称拿到绿卡的某个外国公民，都必须事先得到这个法庭的批准。在美国，此类事情属于联调局的管辖范围，国安局等部门如果要介入，也多半需要由联调局出面申请。据统计，外国情报监视法庭1999年批准的886项监视许可中，大多数都是联调局申请的。[115]

联调局等情报单位提出申请，经外国情报监视法庭批准，随后情报单位开展监视行动，这样一种工作模式，在“9·11”事件之后，开始遭遇到前所未有的质疑。

2001年9月12日，两条“最新”情报送到了国安局局长海顿的桌上，其中一条是“比赛明天开始”，另一条是“明天是行动零时”。[143]这显然是那些策划恐怖袭击的人说的“黑话”。尽管是“黑话”，可此时此刻，这两句话的意思并不需要更多的解释人们就能明白。

这是两天前，也就是9月10日，国安局在阿富汗“基地”组织活动的区域监听到的，但已经于事无补，因为就在前一天，有十几个人完成了他们的“计划”，实施了对纽约和华盛顿的恐怖袭击。这是对国安局工作的莫大讽刺！出现这样的情况，国安局方面将其归因于《外国情报监视法案》的“正常”运作时间太过漫长。的确，从提出调查令申请到最后获得批准，平均要4～6周。虽然在紧急情况下，无须法庭调查令就可以对嫌疑目标进行长达72小时的监视，但这种紧急处置也需要经过国安局情报官同意、国安局律师和司法部律师审批、司法部部长批准实施等环节，一般需要1天到1天半的时间，等待时间仍然比较长。

海顿局长决定在他的权限范围内，绕开《外国情报监视法案》做一些工作。两天后，也就是9月14日，他批准了锁定与恐怖分子相关的国际电话号码的行动计划，但此时局长还是小心翼翼，对于从美国国内打出的电话，仅仅把那些已经掌握的电话号码纳入跟踪的范围。具体任务由特殊情报搜集部（SCS，简称“特搜部”）和美国境外的卫星监视站共同完成。9月26日，海顿又宣布：从即日起，所有打进美国的阿富汗电话号码都具有外国情报价值，应该密切监视。[144]

尽管这两项决定并未超出国安局权限范围，海顿还是在电话里向参众两院情报委员会做了简要汇报，并且向中央情报总监特内特通报了有关情况。特内特立刻就把国安局的这一动向报告给了白宫，副总统切尼让他询问国安局，他们能不能进一步扩大任务范围。海顿局长的回答是：在当前的制度“笼子”里，国安局做不了更多事情。特内特进一步问，如果授予你更大的权力呢？这样的问题，海顿其实早已让下属考虑了，讨论的焦点则渐渐集中到如何填补“国际空白”这个问题上。对此问题，国安局的技术主管做过这样一种形象的描述：

这边国安局站在美国边界上，眼睛向外望，搜寻来自国外的威胁。那边联调局眼睛向内看，搜寻来自国内的威胁。没有人注意正在进入美国的来自外国的威胁，这是国安局应该填补的巨大空白。[144]

1999年，曾有人提出过一种技术方法，利用电话和电子邮件的元数据“建立联系链”。这里要先稍微解释一下“元数据”这个概念。所谓“元数据”，也被称为“描述其他数据的数据”，是与“内容”相对的一个概念。对于一条电子邮件消息，它的“元数据”包括发送者地址和接收者地址，至于电子邮件里写了什么，是这封邮件的“内容”，不是它的“元数据”。与之类似，对于一次电话通话而言，它的“元数据”包括被叫号码、主叫号码，以及通话时长，至于电话里讲了什么，则是这次通话的“内容”。[144]

所谓建立联系链，是国安局内部使用的一个术语，指的是利用一个人或者机构的通信元数据，包括他们发出的或者接收的电子邮件和电话的元数据，搭建与他们有联系的人或者单位的网络图，也就是所谓的社交网络分析。简单地说，就是利用电子邮件和电话通信元数据，发现目标人或者目标单位的通信模式，通过与他们密切联系的人或者机构发现更多值得跟踪的目标。这种方法跟以往的做法完全不同，情报机构不再是针对某些特定电话号码进行跟踪监视，而是需要成批地分析美国国内

电话号码，从中发现与这些号码有着密切联系的线索。但司法部情报政策与审查办公室（OIPR）当即就否定了这种想法，他们告诉国安局：这样的工作属于《外国情报监视法案》规定的“电子监视”，外国情报监视法庭不允许利用美国本土电话号码锁定目标。[144]

在“9·11”事件之后，国安局把这种想法重新提了出来。现在他们有底气“批评”《外国情报监视法案》对监视的渠道开放得不够彻底，不能满足锁定恐怖分子账号和地址的数量要求，更重要的是跟不上恐怖分子变换账号和地址的速度。据统计，从1978年成立到2005年，外国情报监视法庭一共受理了大约1.9万份调查令申请，其中只有5份申请被法庭驳回[143]，他们基本上做到了有求必应。但在国安局看来，《外国情报监视法案》这个“笼子”还是关得太紧，说得好听点儿，叫作灵活性不够，不能适应当前新的恐怖威胁形势。[144]

为了研究反恐新形势下的情报工作，小布什召开了“御前”会议。会上，海顿汇报了他的想法，他希望能突破《外国情报监视法案》的限制，最终实现防患于未然。

小布什：（这样的计划）对我来说很有意义，但是你们不能监视国内的通信。

海顿：是的。我们只监视从国外到国内或者从国内到国外的通信，监视的对象都是我们已经知道或者怀疑的、和“基地”组织有联系的那些人。

小布什：这样的行动合法吗？[145]

听到总统的这个问题，海顿意识到机会来了，他开始向小布什大倒苦水，把自己对《外国情报监视法案》的意见和看法都说了出来。[146]小布什也听明白了，看来必须先“解决”法律问题才能开始行动。但他们选择的解决之道并非修订《外国情报监视法案》，一来这样做需要比较长的时间，二来他们认为这样难免会引起公众的广泛讨论，让恐怖分子对监视行动产生警觉。

副总统切尼想出一个办法：绕过《外国情报监视法案》，采用总统授权的方式开展行动。起草总统授权文件这个任务就交给了切尼的法律顾问戴维·艾丁顿（David Addington）。在海顿的帮助下，艾丁顿很快就把文件起草好了，标题是“授权有限时间内进行特定电子监视活动，发

现并阻止美国国内的恐怖主义行动”。2001年10月4日，小布什总统签字批准了这份备忘录，允许国安局在没有法庭调查令的情况下，对通信内容及其元数据进行监视，包括电话和电子邮件，只要他们有“恰当的理由”相信通信双方中有一方与恐怖活动相关。国安局还有权对由此得到的通信情报进行保存、处理、分析和传播。这就是“总统监视计划”（PSP）的主要内容。[144]总统授权的有效期是30天。再加上其他一些过程中的零碎时间，每隔30～45天就需要小布什重新授权一次。只拿到这样一份授权，海顿心里着实不踏实，他让国安局法务长看看这种授权是否合法。法务长告诉局长，他认为这是合法的。“笼子”终于被打破，国安局可以开始自由行动了！

中央情报总监手上有2500万美元的机动经费，动用这笔经费无须国会事先批准，钱马上就被拨到了国安局账上。经费到位，海顿局长终于打消了最后一丝疑虑——这回要动真格了！他下令在信号情报分局（SID）建立元数据分析中心，开展全天24小时不间断的监视行动。国安局立刻紧锣密鼓地行动起来：指定负责人落实任务和责任、抽调精干力量建立行动团队、腾出办公场地开始挂牌运作、订购50台服务器存储和处理数据。说到这50台服务器，还有个小插曲。由于任务紧急，有关厂商把原计划交给其他客户的服务器挪用给了国安局，如此特事特办，也算是对政府工作的大力支持吧。[144]

从一开始，小布什就知道他授权开展的这项监视行动会引起争议，于是他搬出手中掌握的另外一个法宝：“保密”。

美国有关密级的划分和界定，主要通过总统令或者总统备忘录的形式进行规范，他们把信息分为非密信息和涉密信息。两者最大的区别在于，接触非密信息不需要专门的许可。非密信息又分为两类：一类是公开可以得到的、没有任何限制的信息，情况比较简单；另一类是发布范围受限的信息，这种信息名目繁多，有人统计过，仅美国政府内部就有100多种说法，比如“敏感但非密”、“仅限官方使用”。[147]为此小布什专门在2008年5月发布了一份总统备忘录，试图化繁为简，把所有名目统称为“非密受控”。[148]这份备忘录在2010年11月被奥巴马以第13556号总统令的形式固定下来。[149]

涉密信息按照由低到高的程度，分为秘密、机密和绝密三种。这也是通过总统令的形式规范下来的，曾经多次发布，最近一次是2009年12月发布的第13526号总统令[150]，这次发布与上一次相隔了近15年，

那一次是克林顿发布的第12958号总统令[151]。关于这个第13526号总统令，稍微多说几句。根据这项命令，在美国国家档案馆内设立了国家解密中心，到2013年年底要解密4亿页涉密文件。更重要的是，这项命令确定了一条原则：没有文件可以永远保密。它还规定除了个别情况，不允许文件保密期超过75年。[152]据统计，美国大约有140万人拥有接触绝密信息的许可，曾有人对这么多人接触如此高密级信息的必要性表示质疑[153]，因为这意味着出现泄密的可能性还是比较大的。

美国国防部部长罗伯特·麦克纳马拉（Robert McNamara）曾经发明过一个术语，叫作“比绝密更高的密级”（above top secret）。[154]但不论是中文还是英文，这个说法在字面上都是不能自圆其说的。“比最高更高”，那“最高”就不是“最”高了。把事情说绝做绝，看来古今中外都有这样的陋习，想要“更上一层楼”、进入新境界，只能靠后人绞尽脑汁来打补丁了。

麦克纳马拉想说的其实是，某些涉密信息需要单独管理，仅有少数几个人有权限接触得到。[154]于是，“SCI”闪亮登场。国内不少人根据字面含义，把它译作“敏感隔离信息”，而更好一些的译法可能是“特密专案信息”，这种译法可以更好地体现出它“略高于”绝密的意思。[155]严格说起来，特密专案信息并不是一种“密级”，而是根据需要设定可接触这些信息的群体范围，通常只有很小的一群人可以看到这些信息。换句话说，某份文件可能只是秘密级的，但又属于特密专案信息，那么想看到这份文件，甚至可能比其他一些绝密级的文件，门槛更高、限制更多，也更为困难。

从已经曝光出来的特密专案信息来看，它们基本上都与某种特定的情报源绑定，都有自己的代号。20世纪50年代中期，美国人用“TALENT”作为U-2侦察机的专案代号，这个代号后来扩展到用于覆盖所有航空侦察情报。60年代他们用“KEYHOLE”作为卫星的专案代号，后来又用“TALENT KEYHOLE”作为天基情报平台的特密专案代号。把“KEYHOLE”一分为二，分别针对图像情报卫星和电子情报卫星设立了两个专案，代号是“RUFF”和“ZARF”，放在“TALENT KEYHOLE”之下。[156]也就是说，大的专案下还可以套着小的专案。

在国家情报总监发布的第703号情报界指示中，对“SCI”是这样定义的：

与情报源、情报手段以及情报分析过程相关的涉密国家情报（CNI），以及通过这些源、借助这些手段或者经过这些分析过程得到的涉密国家情报。国家情报总监需要建立正规的使用系统对这些情报加以保护。[157]

对很可能引起争议的“总统监视计划”而言，小布什当然清楚，设立特密专案是最好的保密方式。在开始行动的同时，他就启用临时代号“星爆”（STARBURST）建立起了特密专案。2001年10月底，正式的专案代号被确定下来，叫作“星风”（STELLARWIND，STLW），这个代号长期有效。严格说起来，“星风”实际上并非“总统监视计划”的代号，而是通过这个计划获得的情报信息专案的代号，但很多人并不会严格区分“计划代号”和“专案代号”，就用“星风”来代指“总统监视计划”。

说了这么多，能够接触到“星风”专案信息的到底有多少人呢？据统计，从2001年到2007年1月，共有3033人。这3000多人分为两拨：参与行动的国安局、联调局和中情局人员共2863人，占绝大多数，由海顿局长委托“星风”行动主管批准；国会、外国情报监视法庭以及其他人员只有170人，直接由白宫批准。[144]

“星风”行动得以进行下去，很重要的一条就是执行了严格的保密措施。小布什把这一招几乎做到了极致。他签批的授权文件，由专人送到海顿局长手里，局长直接把它锁进自己办公室的保险柜里。有几次，甚至是局长亲自跑到白宫领取授权文件。这份文件总共只有几个人看到过。即使是政府高层，也只是模模糊糊地了解一点儿情况，因为他们不允许把有关信息透露给他们的法律顾问。就连国家安全事务助理赖斯也不例外。她的律师曾经向艾丁顿抱怨，因为不知情，自己无法向赖斯提供任何“星风”行动方面的法律咨询，没想到，他的这番话得到的答复居然是这样的：

我不会告诉你有或者没有这样一个计划。但是，如果确有这样一个计划，你最好告诉你联调局和中情局里的那些小伙伴，让他们闭嘴。[158]

旧戏重演

为了实施“星风”行动，国安局专门成立了“元数据分析中心”，从其他部门抽调了20多个分析人员、通信人员和软件开发人员，三班倒、轮轴转。局领导对这个机构极为重视，局长每周听取一次汇报，副局长则每天晚上都要到中心去听汇报。[144]

绝大多数国际电话在接通之前，都要经过很小的一组核心交换线路，它们被形象地称作“咽喉”。美国是国际电话进行交换的主要通道。据估计，2003年全球电话交换线路大约承载了1800亿分钟的电话通信，其中有13%（大约230亿分钟）的通信流过境美国，也就是说，既非打入美国，也不是从美国打出，但这部分电话通信由于技术原因需要从美国经过。[144]对于这13%，国安局早已借助第12333号总统令获得了跟踪监视权，这个总统令的发布日期是1981年12月4日。[159]

不仅如此，美国还是当之无愧的世界互联网通信枢纽。互联网通信的规模通常用带宽来代表，用每秒传输的数字信息量来计量，单位是比特/秒（bps）。据估计，2002年国际互联网带宽的总量大概是290吉比特/秒（Gbps），其中只有2.5吉比特/秒的流量没有经过美国。国安局还发现，恐怖分子使用的电子邮箱，无论是美国公司开设还是外国公司开设，其服务器多半在美国。[144]

上文提到，13%的过境国际电话长期处于国安局的监视之下。这次，国安局通过“星风”行动的授权，为监视另外20%进出美国的电话通信扫清了法律上的障碍，更为监视99%以上的互联网带宽扫清了障碍。

元数据是关于数据的数据。没有数据，元数据就成了无源之水、无本之木。所以，为元数据分析中心搜集数据是关乎这个中心生死的头等大事。

国安局计算了一下，这20%（大约370亿分钟）的电话流量，通过三家美国公司就可以基本完成：美国电话电报公司（AT&T）最厉害，占到39%，接下来是微通公司（MCI），占到28%，然后是斯普林特公司（Sprint Nextel），占到14%，三家公司加在一起达到81%。[160]于是，国安局就先从这三家公司入手——这一幕和50多年前的“三叶草”多

么相似！

海顿局长在10月16日发出了第一批信函，放低姿态，讲清意义，告诉这三家公司，国安局和联调局需要他们的帮助，相关情报对于“9·11”事件之后的美国国家安全至关重要，可以帮助政府发现潜伏在美国国内的国际恐怖组织成员，阻止他们发动恐怖袭击。然后，提出明确要求：国安局需要公司对国际电话流量信息进行调查、搜集和处理，并且以机器可读的形式成批提供给国安局等情报机构。给公司吃定心丸也是必须要做的，局长最后在信上说，上述要求已经得到总统授权和司法部部长的批准。从这一天到12月14日，在短短两个月时间里，海顿局长一共发出了147封类似的信函，全面撒网，疏而不漏。[144]

说起来，这并不是国安局第一次和这些公司打交道。要完成监视过境美国的国际通信这一任务，国安局早就和他们打成了一片。其中，美国电话电报公司和微通公司表现突出，帮了大忙。“9·11”事件之后，在国安局还没有得到“总统监视计划”授权的那段时间，他们就主动跑来询问：“我们可以做些什么？”[144]所以，其实并不需要海顿局长讲什么大道理，这几家公司肯定也会积极配合国安局开展工作。

美国电话电报公司在他们的通信中心秘密布置了一个小屋，把主干光缆拉了进去，国安局可以在这个屋子里毫无顾虑和限制地操作。以旧金山为例，公司在交换机房边上隔出了一个105平方米的房间，所有线缆经过分线箱一分为二，一部分维持正常通信，通话双方都不会察觉到被人监视，分出的另一部分则进入了这间641A“秘密小屋”，国安局在屋里装满了各种各样的设备，包括号称“语义流量分析器”的Narus STA 6400、Sun服务器和Juniper路由器等。[161]这些技术设备肯定瞒不过技术专家的“法眼”，所以“秘密小屋”严格禁止其他无关人员进入。公司在西雅图、圣何塞、洛杉矶、圣迭戈的通信中心也是这样设置的。[162]

对于国安局和这些公司之间关系的重要性，他们自己是这样说的：如果这种关系破裂，“美国将白白牺牲它作为全球通信总枢纽的主场优势，国安局的侦听能力将会遭受不可挽回的损害”[144]。

“星风”行动的重任交给了信号情报分局。其中情报分析和报告任务由信号情报分局的分析产品部下属的反恐产品线负责。2004年，参与这项行动的元数据和内容分析人员被单独抽调出来，成立了一个新的部

门：先进分析处（AAD），下设三个组，分别负责互联网元数据分析、电话元数据分析以及对互联网和电话内容的分析任务，数据搜集任务则由数据搜集部下属的特殊情报源行动处（SSO，简称“特情处”）负责，使用电话号码和电子邮件地址等筛选点，把相关信息从搜集到的数据中挑选出来。[144]

尽管在获得“星风”行动授权之前，国安局就具备了搜集海量电话和互联网元数据的能力，但这种能力一直被束缚在《外国情报监视法案》这样的“笼子”里，得不到充分施展。现在，国安局则可以随心所欲地“建立联系链”，把藏匿在茫茫人海中，和嫌疑目标交往过密的人员找出来。唯一的约束就是：所有这一切需要在“反恐”的名义下进行，首要任务是寻找和锁定跟恐怖分子有关的那些人和机构。不过很明显，拥有这种能力后，可以做的事情不会局限于此。

国安局使用多种工具分析元数据、查看分析结果，其中最重要的工具叫作“主干道”，它具有海量元数据的存储、联系链建立和分析功能。“星风”行动启动之初，分析人员只能使用“信号情报导航器”查看“主干道”的输出结果。后来，国安局设计出新的工具，分析的自动化水平进一步提高。特别值得一提的是，“自动联系链提醒”功能。一旦系统发现新的可用的筛选点，就自动显示出来以提醒分析人员注意。为了获得更完整的结果，分析人员会把所有可用的数据都用上，其中包括通过“星风”行动之外的其他渠道得到的数据。[144]

通常情况下，元数据分析人员根据国安局、联调局或者中情局的需求，开展联系链分析工作。他们的需求申请表有两种：一种只针对某个目标的电话号码或者电子邮件地址等具体信息，使用《信息申请表》；另一种则需要得到某个目标的所有联系人，以便通过这些联系人发现更多的调查线索，使用《线索申请表》。元数据分析报告中如果涉及美国人，需要按照专门的规定单独处理。[144]

对通话和电子邮件等“内容”进行搜集和分析是国安局的传统强项。借助于新的行动授权，国安局搜集电话和互联网通信内容的强大能力终于有了用武之地。当然，这一切都必须在“反恐”名义的掩护之下进行。海顿局长非常清楚掌控这些通信内容的意义，他曾经说，这才是“星风”行动的“真正价值”所在。从行动开始到2007年1月，利用这些通信内容，国安局一共提交了490份报告，大约每周两份。那段时间，在国安局搜集的37664个筛选点的相关通信内容中，只有8%涉及美国人，剩下

的都是外国人。国安局对美国人的监视还是比较谨慎的，有一套比较复杂的审批程序。对外国人的通信监视则简单得多，分析人员自己就可以决定。[144]

筛选点信息都存在“星风”行动的地址数据库里。一旦某个筛选点得到了批准，先进分析处的任务主管就会给这条记录打上一个“已在任务中”的标记，然后给特情处的搜集主管发一封电子邮件，要求他搜集有关的通信内容。接下来，搜集主管根据具体的任务类型，启动不同的搜集流程。但不管采用哪种流程，都需要公司的大力支持、密切配合。举例子来说，如果传给搜集专管的是互联网内容筛选点，他可以直接向安装在公司通信中心的设备发送任务指令。搜集到的所有内容数据都将传回特情处，然后利用“混合”系统对语音数据进行分析，通过“灯芯绒”系统对互联网内容进行分析。不管最初的分析请求是哪个单位提出来的，中情局和联调局都会得到所有的分析报告。[144]

前面曾提到，海顿局长原本对于“星风”行动的授权就有些不踏实，他是在听了法务长罗伯特·戴茨（Robert　Deitz）的“专业”意见之后才打消疑虑、下定决心。但法务长意见的依据并不充分也不确定。国安局高层官员想看看司法部法务办公室的完整意见，这原本是再寻常不过的事情，然而出乎他们的意料，白宫方面一直躲躲闪闪、吞吞吐吐。就拿戴茨自己来说，他曾向副总统的法律顾问艾丁顿询问此事，恳求了很久，对方才在保密电话里念了一两段文字。[163]2003年12月，在司法部常任副部长助理帕特里克·菲尔宾（Patrick　Philbin）主持的一次专题会议上，国安局总监察官提出了想看看法务办公室的完整意见。这次会议并没有通知艾丁顿参会，他却不请自来，并且态度强硬，当场拒绝了总监察官的请求。事后总监察官愤愤不平地说：

让国安局去执行秘密行动，却不让他们了解行动的法律依据，实在太奇怪了。[144]

2003~2004年，菲尔宾带着法务办公室主任等人多次前往国安局听取“星风”行动的汇报。回到部里，他们把有关情况向常务副部长小詹姆斯·科米（James　Comey，Jr.）进行了报告。法务办公室主任兼助理司法部部长名叫杰克·高德斯密斯（Jack　Goldsmith），他明确表示“星风”行动的合法性值得怀疑。科米副部长本人是芝加哥大学法学博士，专业傍身、刚过不惑、年富力强，此时刚上任不久。尽管他负责司法部日常管理工作，却被排除在“星风”行动的知悉范围之外。这种情况实在反常，

想必也让他非常恼火。他对这项秘密行动的情况了解得越多，就越怀疑行动的“合法性”——问题恰恰出在互联网元数据搜集上。[164]

步入正轨

2004年年初，小布什心情烦躁，在伊拉克找到大规模杀伤性武器的希望越来越渺茫。而他亲自秘密下令启动的监视行动，原本一直都能顺顺利利地得到司法部部长的签字，顺顺利利地多次获得重新授权继续行动，没想到这一次竟然会在“阴沟里翻船”，遭遇来自司法部的强力阻击。

这次授权的最后时限是2004年3月11日。在到期前一周，科米拜见了他的顶头上司、司法部部长阿什克罗夫特向部长详细汇报了他掌握的情况，两个人商量的结果是：必须重整这项行动，否则不能认为它具备合法性，也不能让它继续开展下去。可仅仅几个小时之后，部长先生突然身体不适，一检查，竟然是胆源性胰腺炎，病情危重，他马上被送进了医院。按照程序，在他住院期间，科米全权代理司法部部长一职。接下来的几天，科米和白宫有关人员进行了磋商，历陈当前的“星风”行动不合法的各项理由。[165]

3月10日，晚上8点左右。科米正在回家的路上，突然接到部长办公室主任打来的电话，说是总统幕僚长卡德和法律顾问阿尔贝托·冈萨雷斯（Alberto Gonzales）正赶往医院，他们是总统派去的。部长正处于术后恢复期，这两人去医院想干什么？科米心里立刻就有了答案。他放下电话，马上给自己的办公室主任打电话，让他迅速通知所有相关人员赶去医院。[165]一场被媒体称作“摊牌”的大戏将就此上演。

科米拨通了联调局局长罗伯特·缪勒（Robert Mueller）的电话，局长是他的坚定支持者。他对科米说：“我们待会儿在医院见。”接着，科米命令随行人员拉响警报器，一路疾驰到了医院。车刚停稳，科米就拉开车门跳了下去，匆忙跑上楼，冲进了部长的病房。病房里黑乎乎的，只看到部长夫人站在床边，部长躺在床上——卡德和冈萨雷斯都还没有到。缪勒也还没有到，但他已经给驻守医院的联调局特工打过电话，命令他们确保阿什克罗夫特部长的安全，必要时候可以采取措施，防止卡德和冈萨雷斯等人硬把科米赶出病房。[166]

在这场争分夺秒的比赛中，司法部在速度上占据了上风。菲尔宾和

高德斯密斯都赶到了。科米找了把椅子，刚在部长床头坐下，门就被推开了。冈萨雷斯走了进来，手里拿着一个信封，卡德跟在他身后。两人礼节性地“关心”了一下部长的病情后就直奔主题——他们要求部长在他们带来的文件上签字。[165]

尽管身体很虚弱，阿什克罗夫特的头脑还是很清醒的，态度也很坚决。他清楚地表明了他的立场：秘密监视行动不合法，必须进行整顿。他还说，自己从一开始就不应该在这个行动计划上签字，白宫划定的知情范围实在太小，根本没有办法了解实情，连找个人咨询此事是否合法都做不到。[167]

病床上的阿什克罗夫特此时已经筋疲力尽，他对冈萨雷斯和卡德说：

我的态度其实无关紧要，我现在不是司法部长，这个人才是。[165]

说到这里，他用手指了指科米。冈萨雷斯和卡德看到事情不可为，只好悻悻而归。这时，联调局局长缪勒也赶到了。科米刚和缪勒聊了几句，卡德就把电话打了过来，他要求科米马上到白宫去。科米是这样回答的：

就我刚才看到的情形，如果没有证人在场，我不会去见你，而且我坚持要总检察长作为我的目击证人……除非我先跟（总检察长）西奥多·奥尔森（ThTheodore Olson）先生联系上，否则我不会去见你。[165]

当天夜里11点，科米和奥尔森一起到了白宫。双方的情绪都比先前在医院时缓和了一些，但结果没有变化——科米没有在文件上签字。“星风”行动本次授权的最后时限已到，白宫方面连流氓手段都用上了，但仍然拿不到司法部的签字，这下彻底无计可施。

关于医院“摊牌”，卡德有着另外一套说法。据他说，他和冈萨雷斯去医院之前，小布什给阿什克罗夫特打过一次电话。在电话里总统是这样说的：

卡德和冈萨雷斯现在和我在一起。我们已经准备好了再次授权（监视计划）这件事情。你过去曾在上面签过字。……我现在就派他们去见你，带着文件，你把字一签，事情就办妥了！[1]

按照卡德的说法，两个人赶到医院，冈萨雷斯对病床上的部长说，“总统刚跟你打过电话，这就是那份文件”。阿什克罗夫特推说自己不是司法部长。冈萨雷斯就说：“既然如此，那就这样吧。抱歉打扰。保重。”然后两人就转身离开了，他们表现得很克制，根本没有强迫部长签字。[1]

相比于前面一种说法，卡德这种说辞的可信度要低得多。即便如此，也没有办法判断哪种说法更接近事实，但无论如何，白宫这次是不能拿到司法部的签字了，他们只有另想办法。

在副总统切尼的授意下，法律顾问艾丁顿重新措辞，起草了一份新的总统令。与上一份总统令不同，这份新命令更加明确地宣称，总统依据自身具有的权力就可以批准执行秘密监视行动。他还去掉了司法部部长签字栏，换上了总统法律顾问签字栏。[167]接下来，小布什就让冈萨雷斯在文件上签上大名，国安局就只能“委屈地”使用这样的授权继续行动了。[144]消息传到科米那里，他怒不可遏，迅速拟好了一封辞职信，其中写道：

在过去的两周时间里……我和司法部一直被要求参与一件完全错误的事情，我们为此进行了斗争。我为司法部，特别是部长的所作所为感到无上光荣。我感到，这是司法部最辉煌的一段时间。然而，我们现在无法纠正那件错误的事情了……为此，我怀着沉重的心情，怀着对我的国家和司法部无尽的热爱，辞去美利坚合众国司法部常务副部长一职，即刻生效。[167]

阿什克罗夫特的办公室主任找到科米，请求他不要立刻把这封信发出去，因为部长本人也准备宣布辞职。同时准备宣布辞职的还有联调局局长缪勒、联调局法务长、中情局法务长等一大批高级官员。[166, 167]

国家安全事务助理赖斯听到了一点儿风声，她建议总统找科米谈一下。赖斯说：“他是个值得尊敬的人，你有必要听听他想说什么。”[168]

一次例行的反恐汇报之后，小布什单独约见了科米。

小布什：我很担心你，你看上去负担很重。

科米：是的，总统先生，我身上的担子的确很重。

小布什：我给你减轻些负担吧，（监视计划）这件事还是由我来决定吧。

科米：总统先生，如果能那样，我很愿意。

小布什：我是行政部门法令的决策者。

科米：那是当然，总统先生。但是，我是司法部可以做什么、不可以做什么的决策者。我已经尽力，但在当前情况下，我不能（把监视计划交给您来决定）。[167]

这次谈话最终不欢而散。“水门事件”中，司法部长和常务副部长为了抗议尼克松总统的某项命令，同时辞去职务，给尼克松以沉重的打击，这被人们称作“星期六夜晚之惨败”[167]。小布什显然不希望这段故事重演。最终，他通过缪勒给科米递了一个口信，司法部可以做他们认为正确的事情。2004年3月19日，他撤销了几天前的授权，并且出面挽留宣布辞职的官员，给国安局一周时间停止批量搜集和使用互联网元数据。随后，他要求司法部和国安局两个部门马上坐下来商量，怎样在《外国情报监视法案》的框架下解决互联网元数据搜集问题。[144, 166]

4个月后的7月14日，这是“星风”行动的一个历史性时刻。困扰行动的互联网元数据问题得到“圆满”解决，外国情报监视法庭签发了第一份指令。[144]从这一天起，“星风”行动不再是小布什和国安局的“私房菜”，至少从形式上来看，“权力”开始重新被关进“笼子”里，监视法庭开始监督这一行动——尽管此时还不能监督整个行动。国安局可以继续批量搜集和分析互联网元数据，但额度会大幅减少，同时接触这些信息的人员被更严格地控制。

其实，司法部对于小布什授权开展监视行动的合法性并没有什么异议。他是美国宪法规定的美军总司令，而且在“9·11”事件之后，国会通过了《使用军事力量授权法》（AUMF），这两个条件都赋予他启动“星风”行动的权力[169]——小布什把秘密监视行动放进了“反恐战争”这个大包里正是利用了这一点。不过，对行动整体合法性的认同，并不代表对每个具体行动内容合法性的认同。事实上，司法部主要是对成批搜集互联网元数据的合法性持不同意见，他们认为应该就此做出一些调整，使得监视行动的法律基础更为坚实。[170]

如果看完科米等人在医院里上演的这出“摊牌”大戏，就以为司法部和白宫，甚至是和小布什之间有什么“深仇大恨”，那就错了——不要忘记，司法部长、联调局局长从来都是总统班底的重要成员，他们反感的主要是副总统切尼及其手下的大权总揽和越俎代庖，以及对司法部门的傲慢无礼，寻找的突破口是“星风”行动在法律方面的某些技术性缺陷。换句话说，如果从一开始，切尼等人能够更虚心地听取来自司法部门的意见，“摊牌”这一幕是完全可以避免的。

互联网元数据只是“星风”行动的四项主要任务之一，其余的三项任务仍然以总统定期授权、司法部部长签字的形式继续开展。但是司法部还在继续工作，努力把“总统监视计划”全部纳入《外国情报监视法案》的框架之下。这项工作一步一步取得进展：2006年5月24日，第一份电话元数据法庭指令签发；2007年1月17日，第一份互联网和电话内容法庭指令签发[144]——官方说法是“总统监视计划”在这一天结束了。[171]

从某种意义上看，这种说法也说得过去。因为从这一天起，原本总统授权的四项任务全部改由法庭指令授权。但在斯诺登交给媒体的一份2009年的政府文件上，页眉处赫然写着“STLW”的字样。[144]前面说过，这正是“星风”的缩写，这就证明行动特密专案仍然被保留，而且对电话和互联网通信的内容和元数据进行监视的四项任务也保持不变，只是行动的授权者和部分行动的范围有所改变，正所谓“换汤不换药”，或者西方人常说的“新瓶装旧酒”。所以，实际上，“星风”行动并没有终止，甚至可以说恰恰相反，行动从这一天开始才完全步入“正轨”。法律专家们给“星风”行动找到了非常“坚实”的法律依据，他们利用《美国爱国者法案》第215条“发明”了一种新的秘密解释，这种司法解释解决了大部分问题，剩下的问题要等到后来的《外国情报监视法案》修正案颁布才能最终解决。

“反恐”一直是“星风”行动最为冠冕堂皇的主题。2006年1月，面对媒体的追问，小布什甚至自创了“反恐监视计划”这个响亮的名字。[172]虽然经历了一系列变迁，美国对恐怖组织，特别是“基地”组织的监视却一刻都没有放松。因此，奥巴马能成功猎杀本·拉登，他应该“感谢”小布什，感谢他启动的“反恐监视计划”。当然，人们有理由怀疑这个庞大的监视行动是不是只做了“反恐”这一件事情。

按照惯例，补充两句科米副部长后来的情况吧。面对科米等人的辞

职，小布什感觉不妙，赶紧承认错误、尽力好言相劝。随着事情平息下来，小布什赢得了连任。在为自己第二个总统任期挑选内阁成员的时候，阿什克罗夫特这样的人显然不能再当司法部长了，科米当然也不合适，“忠贞不贰”的冈萨雷斯是接替部长位置的最佳人选。有了发生在医院“摊牌”的那一幕，科米在司法部里的日子肯定不会太好过，离开司法部成为上策。不过，“是金子总能发光”，2005年10月，他以“总法律顾问”和“资深副总裁”的双重身份正式加盟洛克希德·马丁公司（简称“洛马公司”），完成了从政府高官到商界精英的华丽转身[173]。这是非常具有美国特色的现象，叫作“旋转门”。下一回要说的就是这件事情。

第三回 旋转门

“Booz Allen Hamilton”这个名字原本只有很少人了解和关注。不仅是在中国，即使在美国本土，人们对这家公司也大多只是有所耳闻，对于它在美国情报圈子里扮演何等重要的角色，恐怕打破头也想象不出来。[174]“斯诺登事件”爆发后，这个名字的热度陡增，因为斯诺登告诉记者，自己最后的工作单位就是这家公司，尽管他在这里工作的时间不足半年。很多人把公司的名字译作“博思艾伦”，其实不太准确，应该是“博思–艾伦–汉密尔顿”，但这个名字又稍长了一点儿，还是叫“博艾汉”比较简洁有力。公司方面对于自己的名字被曝光估计非常震惊。更让他们震惊的是，这个毛头小伙子的杀伤力是如此之强，以至于公司股票在斯诺登露面当天放量暴跌2.6%。[175]损失如此惨重，他们在第一时间发表声明，宣布解雇斯诺登，就是自然而言的事情了。

经查明：爱德华·斯诺登，29岁，被本公司聘用不到三个月，被分派到夏威夷的一个团队，约定年薪12.2万美元。因违反本公司的道德条例和政策，（公司决定）从2013年6月10日起，终止其聘用合同。[176]

面对“斯诺登事件”之后的如潮恶评，博艾汉公司的首席执行官拉尔夫·施雷德（Ralph Shrader）站了出来，给自己的员工打气：

我们不能，也不会让斯诺登决定我们的未来……我们为客户做出的贡献决定我们的未来……我们的公司非常非常好，被《财富》杂志评为最值得欣赏的公司，我们还将在这个先进行列里年复一年地保持下去。[177]

大股东“凯雷”

博艾汉公司1914年成立于芝加哥。“二战”期间，德军潜艇神出鬼没，成为美军的心腹大患。美军海军部长威廉·诺克斯（William Knox）找到了这家公司，那时它的名字叫“博思–弗莱–艾伦–汉密尔顿”。公司与海军合作，开发出一套特殊的传感系统，可以捕捉到德军潜艇无线电通信的短促脉冲，进而设计出一种攻击德军潜艇的战术。借助于这套战术，盟军到战争结束时把大多数德军潜艇都击沉、击毁了。这是博艾汉公司与美国政府长期合作的开始。2008年，博艾汉公司把薄利的商业咨询业务剥离出去，单独成立“博思公司”监督运营，剩余的业务部分则继续使用“博艾汉”这个名字并且公开上市，其大股东是私募股权投资公司凯雷集团。[174]美国人对“凯雷”这个名字的发音听上去更接近“卡尔拉”，把它翻译成“凯雷”，也许只是为了听着更响亮一点儿。

相比于博艾汉公司，凯雷集团的历史要短得多。集团成立于1987年，最早的发起人是斯蒂芬·诺里斯（Stephen Norris）和戴维·鲁本斯坦（David Rubenstein），这哥俩儿的第一桶金居然是在冰天雪地的阿拉斯加掘到的。阿拉斯加地理位置偏僻、生活条件恶劣，除了世世代代居住在那里的因纽特人和其他土著居民，很少有人愿意到那里去，属于美国的经济不发达地区。当地土著居民也试着开了些公司，可由于不善经营，亏损连连。为了改善当地的经济状况，经阿拉斯加的参议员提议，在1984年的税收法案中增加了这样一项条款：如果阿拉斯加土著居民开设的公司在某个财年里亏损了，他们可以把这些亏损额转让给那些赢利的公司。赢利公司愿意吗？当然！这些赢利的公司只要给阿拉斯加土著居民支付700万美元现金就可以获得减免1000万美元的税额——这是一件“双赢”的事情，所有人都高兴，而政府除外。精明的诺里斯和鲁本斯坦从这项条款中发现了商机，通过他们的穿针引线，很快就做成了近10亿美元的转让合同，他们从中得到了1%的佣金，差不多就是1000万美元。有了这么一大笔资金撑腰，俩人坐下来一商量，决定开创事业、成立公司，公司的名字也想好了，就是这对搭档在纽约经常光顾的那家高端、豪华、上档次的宾馆——“凯雷”。[178]

兄弟俩还拉了三个人入伙：丹尼尔·达尼埃洛（Daniel Daniello）、小威廉·康韦（William Conway, Jr.）和格里格·罗森鲍姆（Greg

Rosenbaum）。但罗森鲍姆很快就离开了，诺里斯也在1995年离开了凯雷集团。其余三个人则留了下来，都成了亿万富翁。[179]

凯雷集团早期的主营业务还有一项——杠杆收购（LBO）。简单地说，就是动用很少的资金对一家规模较大的公司进行收购，以小搏大，就像杠杆一样。卖方拿到的钱一点儿也不少，买方则只有一条路——让被收购的公司举债，也就是借钱，然后把借到的钱加上实际出的那些钱一并交给卖方。所以杠杆收购也叫“举债经营收购”。理论上看，最终可以形成一个多赢的局面：卖方可以套现自己的股权，买方只用很少的钱就能买下一家公司，条件是背上债务、成为“负翁”，而借钱给买方的银行或者机构则得到了一个“安全”的投资项目。但不要忘了，这只是理论上的。

借来的钱总是要还的：买方必须确保自己收购的公司将来能够赢利，凯雷集团通过撮合这样的收购案从买方那里获得利益也必须看准了。所以，这是一个高风险的行业，当然收益也非常诱人。诺里斯和鲁本斯坦没费多大力气就把过去的上司挖了过来，他叫弗雷德里克·马利克（Frederic Malek），曾经做过尼克松的人事主管。马利克对公司做出的最大贡献之一就是找来了里根时期的国防部部长弗兰克·卡卢奇三世（Frank Carlucci III），而卡卢奇又推荐了老布什的国务卿詹姆斯·贝克尔三世（James Baker III），由国务卿搭桥，把老布什拉进了凯雷集团。[180]通过熟人找熟人，几乎成了凯雷集团的一种发展模式。回忆起自己在集团那段不长的经历，马利克不无得意，他说：“我只不过给公司增加了一点点知名度、拉进来几个‘老家伙’而已。”[181]

马利克确实“谦虚”了。在他的主持之下，凯雷集团在1989年组织一批投资者收购了万豪集团旗下的一家航空餐饮公司，并且把它改名为“凯特瑞尔”。可自从被收购，这家公司就没有盈利过，到1995年终于被再次卖掉。如果说凯雷集团最初为凯特瑞尔花了1个美元，到最后则缩水到只有4美分。[182]从直接经济效益来看，这次收购纯属看走眼了，但马利克在无意中为集团预留了一大笔间接的收益——1990年他把小布什安排进了凯特瑞尔董事会。对此，他是这样说的：

我觉得他（指小布什）一定会在董事会里做得很好。在他父亲的竞选活动中，他的办公室就在我隔壁，所以我很了解他。他当时常来华盛顿，我发现他的商业判断力和实际理解力都很强。我认为他会成为一位好的董事。[183]

当然，这只是马利克的一面之词。小布什到底是不是一个好的董事，鲁本斯坦的看法和他的不太一样：

我们把他（小布什）请进董事会，他在里面待了三年。逢会必到，会上讲了很多笑话，低俗玩笑不少。我后来跟他说……我觉得你在这里不太合适，也许你应该做些其他事情。你没有给董事会带来什么价值，你对公司经营也不太懂。

他说，我正在考虑离开这里，我也实在不太喜欢这里，所以我很可能要退出董事会了。

我说，谢谢。

没想到，从此以后我再也没有见过他。[184]

但不管怎么说，在凯特瑞尔被出售前一年，小布什带着他的股票增值权撤离了凯特瑞尔，既安全又体面。他对此也自有说法：选择离开是为了“集中精力参加得克萨斯州州长竞选”。[182]

除了上面提到的这些大人物，大洋彼岸的英国前首相梅杰[185]、韩国前总理朴泰俊[185]、泰国前总理阿南·班雅拉春[186]和他信·西那瓦[187]、菲律宾前总统菲德尔·拉莫斯[188]等人也都曾在凯雷集团任职。集团赢得“前总统俱乐部”这一绰号绝非浪得虚名。[189]

凯雷在大人物身上投资，那是毫不犹豫的：老布什演讲的出场费标准是每次至少8万美元，梅杰每年28天的“指导”费标准也达到了10.5万英镑。[189]靠着这样的资源，鲁本斯坦和诺里斯一步一步在政治阶梯上越爬越高，最终为凯雷集团推开了财富之门。

成立之初，凯雷集团业绩平平，其业务得以起飞在很大程度上要归功于卡卢奇。卡卢奇1930年出生在宾夕法尼亚州，后来进入了普林斯顿大学，和拉姆斯菲尔德是室友，也是密友。多年后，拉姆斯菲尔德执掌经济机会办公室（OEO），卡卢奇成为他的副手，另一个副手就是后来的副总统切尼。1970年，拉姆斯菲尔德离任，卡卢奇当上办公室主任。1971年他调到行政管理与预算办公室（OMB），先后担任了副主任和常务副主任，而接替他的就是马利克。从1978年2月起，他在中情局当了三年的常务副局长，在1981年2月和1987年11月两次进入国防部，先是常务副部长，然后是部长，一共待了三年多时间。卡卢奇个头不高，

口齿伶俐，深谙讲话的艺术，善于和国会、国务院进行沟通，尤其是在复杂问题出现的时候他总能冲锋在前、独当一面。[180, 190]简而言之，等到卡卢奇离开部长位置时，他已积累了丰富的经验和充足的社会网络资源，很多公司向他伸出了橄榄枝，而部长的选择是凯雷集团。

成功收购BDM国际公司是凯雷集团腾飞的标志。冷战结束后，美国的防务行业持续低迷，福特汽车公司极力想把承担防务业务的福特航空剥离出去。尽管有了卡卢奇，在收购福特航空的过程中，羽翼未丰的凯雷集团仍然输给了比自己声名更盛的劳拉集团。但是，正因为有了卡卢奇，凯雷集团最终也并非一无所获，它们得到了福特航空下属的一家非常成功的防务咨询公司，这就是BDM国际公司。[191]为了收购这家公司，凯雷集团动用了4340万美元，到1997年转手的时候，集团获得了4.54亿美元，收益是最初投资的近10倍。[179, 192]

从收购BDM国际公司开始，卡卢奇就带领着凯雷集团进入防务承包这一神秘领域开展业务。他对这一领域非常熟悉，把退下来的高端人士所能拥有的巨大潜能和余热都激发到了一个新的高度。集团当时的主要业务是收购与各国政府有生意往来的防务公司，经过改造后再瞅准机会卖掉。1998～2003年，凯雷集团一直是美国最主要的15个防务承包商之一。1987～2007年这20年，集团所在行业的平均回报率大约是15%，这已经非常可观，而凯雷集团的年均回报率甚至能达到26%，这是一个非常惊人的数字。集团是名副其实的生财有道、利润丰厚。[179]

集团下属一家公司叫作“联合防务”，主业是生产战车。这是他们1997年从通用动力公司手上抢下来的战利品。在竞标过程中，通用动力出价最高——10亿美元，并且拥有生产战车的经验，很多人都以为联合防务对通用动力来说是一只“煮熟的鸭子”，可就在这个时候，突然出现了一种说法：如果通用动力把联合防务买下，他们可能将面临反垄断官司。这样的声音越来越大，也越来越逼真，最后的结果出人意料，通用动力退出，联合防务被凯雷收入囊中，他们给出的价码是8.5亿美元。[193]

联合防务一门心思开发一种叫作“十字军战士”（Crusader）的自行榴弹炮，它自重60吨，再加上一个50吨的补给车，整体形态硕大、行动笨拙，华尔街把它称作“恐龙”。随着冷战结束，这样一种基于“大规模陆军对抗”的设计思路，即便是小布什也提出了质疑，他在竞选演讲中指

出，现在需要的陆军“不再是看它的数量和规模，而要看它的机动程度和速度”。为了保住这个项目，凯雷集团展开了大规模的游说活动，最终争取到了宝贵的时间，拿到了他们想要的分红。[193]国防部部长拉姆斯菲尔德也不看好这个“十字军战士”，悄悄把它拉进了“黑名单”，作为首先被考虑撤销的项目之一。但他隐瞒了这个决定，因为他的好友卡卢奇和凯雷集团正在运作联合防务上市的事情。直到公司顺利上市6个月之后，拉姆斯菲尔德才宣布“十字军战士”项目正式下马，但集团此时已经在市场上圈到了2.37亿美元。[194]而且，就在联合防务宣布“十字军战士”项目下马的同一场新闻发布会上，他们透露，刚刚拿到了一个新的火炮合同，这种装备很像“十字军战士”，但比它轻得多，只有不到20吨。[195]

在英国，集团的生意也开展得非常顺利。英国国防部下面原来有一个“国防评估研究局”（DERA），2001年这家单位一分为二，一部分改名为“国防科学技术实验室”，留在国防部内，另一部分改名为“奎内蒂克”，实行公私合营，英国国防部保留56%的股份，凯雷集团收购了34%的股份，但借助于一项特殊协议，集团拥有了51%的股权。换句话说，奎内蒂克的实际控制者是凯雷集团。靠上凯雷这棵大树，奎内蒂克一口气收购了五六家中等规模的情报业务公司，也变成了一个工业–情报复合体。还记得“灌篮”总监特内特吗？他后来成为这家公司的非执行董事，也是董事会里唯一一个美国人。[196, 197]为了收购奎内蒂克的股份，凯雷集团大约支付了1.5亿英镑，然后它用了4年时间一点一点卖掉了所有股份，一共挣到了2.5亿英镑。[198]

2004年，迈克尔·摩尔（Michael Moore）拍了一部纪录片，叫《华氏9·11》（*Fahrenheit 9/11*），该片在法国戛纳电影节上出尽了风头，最终把金棕榈奖收入囊中。摩尔取这样的片名是向小说《华氏451》致敬。那是1953年出版的一部反乌托邦小说，作者是雷·布雷德伯利（Ray Bradbury），他认为纸张的自燃点是451华氏度，故取此名。小说里有一个重要情节：将来某个时候，书籍在美国会被当作非法制品，消防员的任务不是灭火，而是烧书，发现一本就烧掉一本。顺便说一句，因为其影响力和重要性，这部小说在2012年被美国国会图书馆评为“塑造美国的图书”之一。[199]摩尔根据自己对这本书的理解，为自己的电影设计了一句宣传口号，叫作“自由燃烧的温度”[200]。在这部电影里，布什家族和拉登家族之间的一根黑线被晒了出来，这根黑线就是凯雷集团：老布什是集团高薪聘请的顾问，拉登家族则是集团的股东之一，持有集

团200万美元以上的股金，当然，拉登家族只是非常微小的股东。这些事情在这部电影拍摄之前就有人披露，只是没有造成这么大的影响。

比如，2003年就有一篇文章公开写道：就在“9·11”事件当天，凯雷集团在华盛顿特区召开了投资者年会，老布什和詹姆斯·贝克尔等贵宾出席了这一会议。到场嘉宾里还有一个名叫沙非克·本·拉登（Shafiq bin Laden）的沙特人，事后确认这个人竟是本·拉登的哥哥。更让普通美国人气愤的是在恐怖袭击后飞行控制异常严格的情况下，十多个拉登家族的成员居然还能神不知鬼不觉地飞离美国，不知道采用了什么办法。[201]

人们通常所说的本·拉登，全名为奥萨马·本·穆罕默德·本·阿瓦德·本·拉登（Osama bin Muhammad bin Awad bin Laden）。其实他的民族并没有姓氏的概念，西方人根据他们自己的拼写习惯，把“本·拉登”当作了他的姓氏，并且在大多数场合称呼他为“本·拉登”，严格说起来这是一个错误。他名字的大意是说：我是拉登的儿子阿瓦德的儿子穆罕默德的儿子奥萨马。所以拉登其实是他曾祖父的名字、阿瓦德是他祖父的名字，依此类推。但这事儿也不能全怪西方人，为了和西方人做生意，他的家族把“本·拉登”作为家族企业的名字，某种程度上也加深了这种误解。本·拉登比较正式的简称应该是“奥萨马·本·拉登”。

本·拉登算得上是其家族的叛逆，早在1994年就被逐出门庭。[202]他的生父先后结了22次婚、生了54个孩子。他的继父又带来了4个孩子，那个被记者挖出来的“沙非克”哥哥是这个继父的孩子，把他和本·拉登联系到一起实在有点儿牵强。至于全家逃离美国，避一避风头本无可厚非，可难免让人感觉他们有些“做贼心虚”。

《华氏9·11》像一根导火线，把美国民众对本·拉登的深仇大恨、对伊拉克战争的满腹怨气、对投资集团巧取豪夺的无比愤慨全点燃了，对凯雷集团的声誉有巨大的杀伤力。对凯雷集团来说，这无疑是一件非常糟糕的事情。自“9·11”事件发生以来，集团就一直在清理整顿，这个时候更是拿出了刮骨疗毒的勇气，大刀阔斧变革、修补形象：第一板斧是“清理门户”，让拉登家族拿钱走人；第二板斧是“婉退权贵”，拜会老布什和梅杰，动之以情、晓之以理，向他们说明为了避免企业形象受到损害，不再聘请他们担任高级顾问等，并且解除了卡卢奇集团董事会主席的职务，转而让IBM公司（国际商业机器公司）前任首席执行官郭士纳（Louis Gerstner）接任。当然，最艰难的是第三板斧“转移方向”，实

施多样化战略，不再过分依赖国防业务挣钱，同时大规模抛售手中持有的防务公司股份。到2005年，凯雷集团在美国国防承包商的排行榜上迅速下滑到100名之外。[179]在这种情况下，集团大肆收购具有强烈政府背景，特别是在防务和情报圈子里摸爬滚打多年的博艾汉公司的股份，显得有那么一些不同寻常。

麦康奈尔其人

打开博艾汉公司的网页，在公司领导人页面，有一个名字，“麦康奈尔”，他是公司董事会副主席之一。单看照片，这个人显得有点儿学究气，有一句古话说“人不可貌相，海水不可斗量”，他其实并不简单：1992~1996年，他担任过老布什和克林顿任期内的国安局局长，2007年接替尼葛洛庞帝，成为第二任美国国家情报总监。1997~2006年这10年间，他一直是博艾汉公司的高层领导。

“情报工作”实在不是尼葛洛庞帝的长项。在担任国家情报总监之前，他的职务是美国驻伊拉克大使，从总监位置上退下来之后，他又回到了国务院，那里才是他更熟悉、应对更自如的环境。相比之下，约翰·麦康奈尔（John “Mike” McConnell）算得上是情报界的“老同志”了。他出生于1943年，家境贫寒，靠助学贷款和打工完成了学业。为了省钱，有个学期他甚至只能在学校体育馆的储藏室里借宿。[203]越南战争期间，他参加了美军，后来到美国海军第七舰队总部横须贺从事反情报工作，20世纪70年代成为美国海军驻扎在波斯湾和印度洋军舰上的情报官，指挥了海军在中东的情报行动，成为海军情报长官的主要助手。[204]他的同事都会提到他的稳重克制和彬彬有礼，以及很少发脾气。但也有人说，他的礼貌和南方口音只是表象，必要的时候他也会发力[205]——大概就属于我们常说的“绵里藏针”的那一类人。

在第一次海湾战争中，海军上校麦康奈尔被参联会主席鲍威尔选作情报官，但对他能否胜任，鲍威尔心里并没有底。因为他的专长是技术情报，对地面作战并不熟悉。鲍威尔后来回忆说：“我当时认为那个夏天不会发生什么情况，才让他当我的情报官。”

一天，麦康奈尔向鲍威尔报告：伊拉克部队正在科威特边境集结。他原以为鲍威尔会问“他们有多少个师”，可没想到鲍威尔的问题是“他们有多少个机动旅”。麦康奈尔一下就懵了，因为他甚至连什么是机动旅都不知道……他老老实实地向鲍威尔坦白：“我不知道答案，但可以去把这些基本情况搞清楚。”鲍威尔听到这样的回答并没有不高兴，他对麦康奈尔说：

把你知道的情况告诉我，再把你还不知道的情况也告诉我，最后再把你预料的情况告诉我。要永远把这三种情况区分清楚。[203]

这是参联会主席对情报官的要求。在此后几周的时间里，麦康奈尔随身携带了记忆卡，恶补陆军术语。他下的这番功夫很快见到了成效，不久他就掌握了地面作战知识，可以在鲍威尔面前自如地汇报情况，甚至可以带一点儿表演的性质，就像“周六夜场秀”那样。这样的汇报让参联会主席很是欣喜，于是汇报成为麦康奈尔每天的“必修课”。伊拉克入侵科威特前24小时，麦康奈尔对他们的意图明确给出了判断，事后证明他的结论非常正确，这件事让国防防部长切尼很是欣赏。[203]因为获得了这两位“首长”的赏识，麦康奈尔的人生从此走上了一条高速路。1992年，国安局局长的位置空了出来，鲍威尔和切尼都想到了他，但按照规矩，那是个三星中将级别的位置，而麦康奈尔晋升为一星准将才不过9个月。为了能让他接班，已经升任副总统的切尼命令国防部特事特办、破格提拔，这在美国海军历史上非常罕见。这次破格提拔也成为体现麦康奈尔与切尼等人结下的深厚“友谊”的标志性事件之一。[204]

根据博艾汉公司的介绍，麦康奈尔是最早把“信息保障”放在战略高度来看待的美国政府高官之一，他对信息安全问题非常“重视”。在他的领导下，国安局借助加密手段，在白宫、国防部、情报以及外交部门之间建起了一条安全通信渠道。[204]

1993年，美国电话电报公司生产出了一种电话加密装置，采用的是“数据加密标准”算法。此举一出，情报和执法部门原本可以轻松进行的电话监听，突然变得很难开展。这可急坏了政府部门，对国安局来说更是一场噩梦，因为从此以后，任何人（包括美国的“敌人”）都可能使用这种加密手段保护自己的秘密。有人甚至预想出这样一个场景：

白宫的高级技术决策者们经常有这样一种恐惧：将来的某一天，有人在世界贸易中心双子塔里放置了偷来的原子弹，摧毁了半个曼哈顿。白宫只能向国会紧急调查委员会解释：尽管政府监听了恐怖分子的通信，但由于对方使用了强加密手段，他们无法掌握对方的具体动向。[206]

这段文字登在了《纽约时报》上，时间是“9·11”事件发生的七年前，和后来发生的实际情况有几分“神似”，袭击目标没变，仍是世界贸易中心双子塔，幸运的是，恐怖分子没有偷到原子弹，他们改用了民航

客机。

为避免“敌人”利用加密手段逃避监听，副总统阿尔·戈尔（Albert Gore， Jr.）主持专题会议研究对策。会议决定由政府出面把美国电话电报公司生产的加密电话全都买下来，这笔订单当然是秘密的。在此基础上，麦康奈尔和国安局提出了一个更“高明”的想法：和美国电话电报公司再签一份合同，让他们对加密电话进行改装，换上由国安局开发的一种特殊芯片，代号为“羊毛剪（CLIPPER）”，编号“MYK78T”。说它“特殊”，是因为芯片上预留了可以被美国政府随时打开的“后门”。利用同一批电话居然可以签订两份合同，天下居然有这样的“美事”，美国电话电报公司当然不会拒绝！打开“后门”的密钥被一分为二，政府“委托”财政部和商务部分头保管。当然，国安局也具有随时打开“后门”的能力和权力——这是必须保证的。麦康奈尔等人还积极推动立法，要求所有政府机关都使用这种特殊芯片，并且逐步向全社会推广。[207]

考虑到密码技术的重要性，美国政府一直禁止出口高技术的密码产品。以“数据加密标准”算法为例，据统计，尽管1994年国际市场上已经有150多种硬件和软件使用了这项技术，但美国政府仍然禁止商业公司出口这项技术，这使得这些公司的相关产品在国际市场上缺乏竞争力。[206]针对这一问题，麦康奈尔和国安局提出的“折中”办法是：积极鼓励商业公司出口带有这种“羊毛剪”芯片的、从某种程度上来说很“先进”的密码设备。对于其先进性，麦康奈尔是这样说的：国安局为这款芯片设计的加密算法“Skipjack”比“数据加密标准”算法强大1600万倍。[208]他的这番话应该补上这么一句才完整：除了有个“后门”，它基本上没有缺点。

一想到控制自己的生意秘密和生活隐私的那把钥匙放在别人手里、由别人保管，恐怕没有人会觉得心里踏实——哪怕这个“别人”是政府部门。更何况这么做也并非必须。

无论加密解密，都需要使用密钥。按照传统的方法，通信双方会使用相同的密码。但问题的关键是：通信双方如何知道这个密钥？能想到的只有两种办法：双方当面商量好密钥，或者通过可靠的第三方（例如信使）传递密钥。1976年，斯坦福大学的贝利·迪菲（Bailey Diffie）和马丁·赫尔曼（Martin Hellman）发表了一篇影响深远的论文《论密码学的新方向》，引入了一种新的理论。简单来说就是，通信双方的密钥都分为“公钥”和“私钥”两个部分，公钥对所有人都公开，私钥则对外保

密。运用特殊的数学原理，可以保证甲方用乙方的公钥加密信息，只能用乙方的私钥解密，从而在没有第三方参与的情况下，实现了密钥的交换和管理。麻省理工学院的三个数学家罗纳德·瑞维斯特（Ronald Rivest）、阿迪·沙米尔（Adi Shamir）和伦纳德·艾多曼（Leonard Adleman）则开发出了一种系统，把迪菲和赫尔曼的理论变成了现实。他们用三个人姓氏的首字母来命名这种新的系统——这就是著名的“RSA”。后来他们三人索性“下海”成立了一家公司，专门售卖他们发明的这种新系统，公司的名字就叫作“RSA数据安全公司”。[206]加密解密历来是国安局的强项。在很长一段时间里，国安局代表着美国密码技术的最高水平，无人匹敌，但这种局面从此一去不复返了。

推广“羊毛剪”芯片的计划一经公开，立刻遭到来自各方的怀疑、抨击和反对。贝尔实验室的马修·布雷兹（Matthew Blaze）博士更是发现芯片本身存在严重的漏洞[206, 209]，这使得更多的人质疑这种“羊毛剪”芯片，因为它看起来既不可信也不可靠。美国政府被迫在1996年取消了这项不得人心的推广计划，“羊毛剪”芯片只用于美国电话电报公司的TSD-3600-E这一款电话的加密装置上[210, 211]——布雷兹博士甚至还在Flickr网站上公布了这种芯片和电话加密装置的照片。[211, 212]诸位也可以用一分钟检查一下自己的电话，看看有没有“中头彩”！

当然，这只是一个玩笑。“中头彩”的可能性极小，因为毕竟这是20年前的一款加密装置，即使曾经用过，也很可能早被淘汰了。麦康奈尔的这种“创意”却没有被淘汰。

2007年8月，微软公司的一位年轻程序员在密码年会上做了一次发言，宣布他和同事发现有一种被用来生成随机密钥的算法，可以被植入“后门”。这是一种双椭圆曲线伪随机数生成算法，叫“Dual_EC_DRBG”。他的这次发言只有短短几分钟，当时并没有引起公众更多的关注。[213]几年后，路透社披露，国安局曾秘密支付给RSA公司1000万美元，让他们把这种带有缺陷的算法作为BSAFE软件默认的随机数生成算法。RSA公司的BSAFE软件是供程序开发人员使用的工具包，有Java和C语言两种版本。[214]开发者可以把这个工具包嵌入自己的程序，实现加密解密、安全传输和证书授权等功能，但如果使用了这种带有隐患的伪随机数生成算法，系统的安全措施将形同虚设，国安局可以在未授权的情况下轻松进入这些系统。

麦康奈尔从国安局局长的位置退下来之后，开始了他的“旋转门”经

历——先是进入博艾汉公司做起了资深副总裁。正当他开始琢磨国家情报总监位置的时候，“贵人”切尼再次很有默契地伸出有力之手，把他扶上了总监之位。[204]于是，麦康奈尔又转回了政府机关，并且成为美国情报界的头号人物。[204]两年之后，他刚刚任满，博艾汉公司又急切宣布总监先生将要回到公司，继续做资深副总裁[215]，很快他又变成执行副总裁[216]，再后来升格为董事会副主席，跻身博艾汉公司的最高领导层。[217]

麦康奈尔在政府和公司之间的“旋转”如此自由、如此高调，自然招致了很多批评。有赖于他和情报部门人员的深厚关系，以及他拥有的丰富人脉，他常常成为公司在华盛顿的形象代言人。他的努力没有白费，从总监的位置上退下回到博艾汉公司后的第一年，他就挣到了410多万美元，成为公司“快速扩张的赛博业务”的领导者。[218]有人言辞犀利地抨击道：“还没有人像他这样令人震惊又毫无廉耻”。[219]说这话的人名叫格伦·格林沃德（Glenn Greenwald），他原本在媒体圈里就小有名气。几年后斯诺登慕名与他联系，通过他的文章曝光了“棱镜”计划，更使他声名鹊起。这些事情随后还会仔细讲述。

正因为麦康奈尔有如此深厚的商业公司背景，他的每番言论总能让人听出些弦外之音。在国家情报总监的就职典礼上，他说了下面这段话：

我绝大部分的职业生涯是在情报界度过的，主要工作是为决策者提供合适的信息，在合适的时间、以合适的形式。今天的回归令我非常兴奋。

幸运的是，过去10年离开政府之后的工作经历，使我能够从一个战略家和顾问的角度关注国家安全部门和情报单位。所以，从很多方面来看，我从来没有离开过。[220]

正是在他的这种“关注”之下，博艾汉公司才得以参与小布什反恐战争里的许许多多高度敏感的情报任务。[204]对于他讲的“从来没有离开过”，就有人评论说，无论身在政府还是身在公司，他代表的都是同一个利益集团，投身的是同一项事业：把国家的情报和监视任务外包给私营公司，牟取暴利且远离监管。[219]

麦康奈尔就任国家情报总监一年之后，《外国情报监视法案》（修

正案）正式颁布。根据这项法案，参加总统授权、政府认可的监视行动的通信公司都将获得豁免。也就是说，哪怕这些监视行动被判定为非法，所有参与行动的通信公司都不会被问责。请注意这里用的修饰词是“所有”。得到豁免的不仅是现在参加行动的这些公司，还包括历史上曾经参加过行动的那些公司——只要这些公司还存在。这被称为“追溯豁免”[221]。商业公司真正体会到了政府的“关心”和“爱护”，便更加死心塌地、心甘情愿地和政府坚守在一条船上，成为一个利益共同体，一荣俱荣、一损俱损。很少有人知道，在这部修正法颁布前几个月，国安局已经悄悄启动了一项新的、极为秘密的监视行动，这一次他们的合作伙伴是互联网公司。有了新法案撑腰，商业公司就再也没有什么后顾之忧了，即使那些号称“不作恶”的公司也不必良心不安，可以欣然从命。这就是“棱镜”计划。

离开总监位置一年后，麦康奈尔在《华盛顿邮报》上发表了一篇署名文章，文章这样写道：

美国正在参与一场赛博战争，并且在这场战争中正处于劣势……我们需要企业、社会和政府展开对话，迎接在赛博空间里面对的挑战……我们成为冷战中获胜的一方，靠的是强劲的资金投入……让我们在赛博安全方面也这么做吧。[222]

普通人看到这些文字，很可能认为这位已经离任的政府高官是在诚心诚意地为国家出谋划策，很难想到这些话背后隐藏着巨大的利益。可别忘了，博艾汉公司赋予麦康奈尔的职责就是打理“快速扩张的赛博业务”。[223]就在这篇文章发表两周之前，公司发布了一份宣言书，题为“打造赛博力量之路：数字时代控制风险、抢抓机遇”，文中指出：历史上，那些利用新技术、创立新行业的国家都实现了经济转型、社会发展，成为国际舞台上富强的领导者。赛博技术就是这样的新技术。[224]

只有把这两份资料联系在一起，才能稍微读懂麦康奈尔这番话的真实含义：如果政府舍不得在赛博技术方面投入资金，就会在赛博战争中被他国打败；反之，只有舍得投入，美国才有可能继续成为“领导”国际社会的强者。“强劲的资金”应该投给谁呢？当然是博艾汉这样的“优质”合作伙伴。2013财年，博艾汉公司取得了2.19亿美元的净收入，麦康奈尔刚回公司的2010财年，净收益只有2500万美元。[218]这才是名副其实的“快速扩张”。

为什么说博艾汉公司是“优质”伙伴呢？这里有四个关键词。一是“感情”，在“9·11”事件中，有三名博艾汉公司的员工在五角大楼的工作岗位上殉职，用他们的生命深化了公司与军方和政府之间的“深情厚谊”；二是“资格”，博艾汉公司有1万多名员工拥有TS/SCI许可，也就是“绝密/特密专案许可”，这是情报界最高级别的涉密许可，这么多员工有资格参与高密级的工作，意味着公司有一支在“政治上”非常可靠的队伍；[204]三是“经验”，早在10年前，麦康奈尔离开国安局之后，他就带领着赛博安全团队为博艾汉公司赢得了近3亿美元的合同，承担政府“关键基础设施保护”的相关任务。[203]但这三个关键词还远远不能代表博艾汉公司的全部优势，他们最大的优势源自第四个关键词：“旋转门”。

“国家安全有限公司”

算起来，博艾汉公司是一家不折不扣的“百年老店”了。公司2013财年收入为57.6亿美元，其中99%来自联邦政府。往前追溯，2010~2012财年，博艾汉公司通过为政府部门提供外包服务获得的收入基本上保持在总收入的97%~98%。原来，它的客户几乎只有一个，那就是美国联邦政府。再往下看，公司近1/4的收入，也就是13亿美元，来自美国情报单位，过去两年里这一比例基本维持不变，他们的主要工作是为相关单位的战略规划提供关键支撑、改进情报信息的处理流程等；公司有超过一半的收入来自美国军方，任务主要涉及陆军地面情报系统、物资运送系统等。[174, 225]

中情局前副局长琼·邓普西（Joan Dempsey）女士曾把博艾汉公司称作“影子情报圈”，因为在这家公司里不时能碰到曾在情报和军队系统或者政府部门担任要职的人。具有讽刺意味的是，就在她讲完这番话15个月之后，邓普西自己也未能免俗，进入博艾汉公司工作[174, 204]，成为公司负责防务情报业务的执行副总裁[226]。

说到执行副总裁，公司网站上显示的人员数目是36个，有点儿夸张吧？要知道公司的资深副总裁总共有51个。最夸张的是副总裁数量，比执行副总裁和资深副总裁加起来还要多，居然达到了90个。此外，还有13个资深执行顾问。由于没有找到公司正式发布的组织结构图，所以这些“高层”之间的关系只能靠猜测了。公司的执行副总裁是仅次于公司总裁的第二层级高管，资深副总裁比执行副总裁低一个层级，副总裁比资深副总裁再低一个层级。至于资深执行顾问，大致可以理解为退居二线、不承担具体工作的“领导”。

美国有些奇怪，总有一些人能够在政界、工商界和学术界这几个不同的领域里往来穿梭、畅行无阻。这就是所谓的美国式“旋转门”现象。商业公司借助卸任的高官拿到大量的政府订单，作为交换，这些高官在公司里享受高薪。这也可算是一种“双赢”。

前面提过的凯雷集团，也是一家比较典型的“旋转门”公司。发起人之一的鲁本斯坦就有在政府高层任职的经历。他在27岁就当上了詹姆斯·

卡特（James Carter, Jr.）总统的国内政策副助理，曾经坚信作为一名公务员拥有无上光荣。在卡特败给罗纳德·里根（Ronald Reagan）之后，鲁本斯坦离开政界，做了几年“有失身份”的游说生意，后来创建了凯雷集团。经过慎重考虑，他把集团总部设在华盛顿，而不是其他公司通常考虑的纽约或者芝加哥。公司选址在联邦政府的门口，这一举动的意图非常明显，就是为了方便自己利用广泛的政府社交资源做生意。新闻媒体把他们这类人称为“关系资本家”。[178]经过20多年的打拼，鲁本斯坦终于走向成功。2012年，他位居《福布斯》杂志评选的全美富豪排行榜第250名，身家达19亿美元，[227]成为“旋转门”内外的人们羡慕、嫉妒和追逐效仿的对象。

还记得第一回里说过的“9·11”事件委员会报告吧。撰写者曾在这份报告里痛心疾首地指出：冷战后，美国情报圈一夜之间失去了最大的敌人，经费被削减、编制被压缩、力量被削弱。[33]但反恐新形势时间紧迫，靠情报圈子自己培养队伍，时间上不允许，唯一可行的办法只能是依靠社会力量，也就是依靠私营公司的力量完成反恐情报的搜集和处理任务。

“9·11”事件之后，一批原本并不起眼的私营公司迅速崛起，博艾汉公司作为其中的佼佼者，成绩更是显得抢眼。公司收入从2001年的8.4亿美元增加到2013年的57.6亿美元，翻了几番。[228]总体来看，2008～2012年，美国政府外包给私营公司的项目经费略有波动，但大致稳定在2500亿～3000亿美元之间，而外包给博艾汉公司的经费则稳步增长，公司排名也从第25名一步一步攀升到第14名。[229]这样的发展速度着实让诺斯罗普·格鲁曼公司（简称“诺格公司”）这样的大公司眼红。

说起诺格公司，就不能不提F-14“雄猫”战斗机、F/A-18“大黄蜂”战斗攻击机、RQ-4“全球鹰”无人机、B-2“幽灵”战略轰炸机、“尼米兹级”航空母舰，这些先进的武器装备都出自这家公司，它在全球防务界给人留下一种“硬汉”的印象。就是这样一家公司，2002年收购了长期承包中情局和国安局防务项目的天合汽车公司，2007年收购了埃塞克斯公司，再加上早几年吞并的DPC技术公司等，这些并购使诺格公司在比较“软”的情报圈子里也成为一个举足轻重的角色。[230]还记得前面提过的BDM国际公司吗？凯雷集团从劳拉集团手里抢下了这家防务咨询公司之后，于1997年转手卖掉，而接手的买家就是天合汽车公司。[231]

通用动力公司的情况也差不多。2001～2010年，这家公司先后吞并

了11家运营卫星、信号情报、地理空间情报、监视和侦察等相关业务的公司。2003年，通用动力拿到了国土安全部数亿美元的合同，为国土安全部新设立的部门服务，包括国家行动中心、情报与分析办公室、安全办公室等，公司员工从事的工作从确定调查对象到接听电话，一应俱全。公司情报信息相关部门的收入，从2000年的24亿美元激增到2009年的108亿美元，超过公司总收入的1/3。[232]

“9·11”事件之后，美国情报界“主要依靠社会力量”的工作方针着实养肥了一批“旋转门”公司。据彭博社估计，2013年，美国情报预算有70%被外包给了商业公司。[174]《华盛顿邮报》形象地把这些公司统称为“国家安全有限公司”。[232]当然，获益最多的还是公司高层。以博艾汉公司为例，其最高管理层的五个人2013年的平均年薪达到了400万美元。[233]

和“旋转门”相生相伴的还有一种具有美国特色的现象，叫作“游说”。这在美国被认为是公司企业、民间资本影响政治的一种合法手段。当然游说的目的十分明确，就是希望能够从政府那里得到回报。但奇怪的是，博艾汉公司对此事一点儿都不积极，他们在游说方面的投入极少。博艾汉公司有迹可循的唯一一笔游说费用支出是2002年的4万美元。[234]与它的竞争对手相比，这绝对可谓微乎其微。

在博艾汉公司的一份年报里，它把自己的竞争对手分为三类：第一类是政府服务提供商，包括L-3通信、凯西国际、曼太国际和SRA国际等公司，游说费用最高的L-3通信公司1998～2012年支出3812.1万美元，最低的SRA国际公司也支出了216.5万美元；第二类是大型防务承包商，包括诺格、洛马、通用动力和雷声等公司，这类公司出手阔绰，花销最高的诺格公司支出了1.91亿美元，最低的雷声公司也支出了7404.7万美元；第三类是杂类服务提供商，有埃森哲、科应、计算机科学（简称“计科”）、德勤等公司，这类公司在游说方面不吝花费，花销最高的埃森哲公司支出3.63亿美元，最低的德勤事务所也支出了248万美元。[233]

可即便在游说方面不积极，博艾汉公司仍然能够不断得到联邦政府的大量合同，这反映出这家公司与联邦政府、军方以及情报界的广泛而深厚的联系。除了上面提到的麦康奈尔，现任美国国家情报总监詹姆斯·克莱伯（James Clapper, Jr.）也曾做过这家公司的副总裁。

说到与国安局的关系，博艾汉公司有9位副总裁以上的公司高管曾

经在国安局工作过。有三位值得一提。第一位叫詹姆斯·艾伦（James Allen），他曾经担任国安局信号情报分局分析产品部副部长，最早在海军服役，当过密码军官和水面战军官，现在是负责信号情报技术分析服务和开发应用的资深副总裁。[235]第二位叫理查德·威尔海姆（Richard Wilhelm），曾是国安局第一任信息战部门主管，早前曾是海军情报军官，担任过沙漠风暴行动中对伊联合情报中心的指挥官，现在是公司负责美国情报单位业务的执行副总裁，之前负责过公司的情报分析业务。[236]第三位叫泰瑞·汤普森（Terry Thompson），他曾是国安局支持业务分局的副局长，现在是负责中东地区情报分析和赛博安全业务的副总裁。[233, 237]

博艾汉公司跟中情局的关系也不一般，公司有7位高管曾在中情局工作过，其中就有前面提到的邓普西。[233]平心而论，一个女人能够晋升到她这样的位置，相当不容易。公司公开的简历上并没有提到她的学历，现在能知道的是，她早年曾作为预备役军官在海军密码部门工作，后来逐步成长为国防部的高级文官，担任过国防情报局常务副局长。1997年，因为在首次进行的四年一度防务评审等工作中的突出表现，邓普西获得“防务杰出文官奖”；1998年，被“灌篮”总监特内特选中，她当上了中情局副局长；再后来回到国防部，她先后担任负责情报安全的助理部长帮办和负责C3I的代理助理部长。[204, 226]

对于自己一路成长进步的最大经验，邓普西的总结是“敢闯敢干”。作为助理部长帮办，邓普西面临的主要问题是如何落实好国防部的“信息行动”指令。这是一份“超前”的指令，规定了赛博行动的指导方针，而当时很多人连赛博是什么都还不理解，由此可见落实这样一份文件的难度。“管理什么、如何管理、由谁来管理，对于这些问题，大家争论不休”，邓普西迎难而上，“大概用了一年时间就把这一切都搞定了”。面对人们对她“旋转门”经历的质疑，在记者面前，邓普西这样说道：

我真希望，如果当时能在政府工作生涯的某个时点到公司里转一下就好了。那样的话，我就能更了解公司是怎样运作的，更清楚从公司角度看到的政府是什么样的，也就能成为一名更好的政府高级官员。[238]

上面提到的7位前中情局高官现今都在公司中任职，但并不包括已经离开博艾汉公司的詹姆斯·伍尔西（James Woolsey, Jr.）。这位先生在克林顿执政时期当过近两年的中央情报总监，2002～2008年是公司的

资深副总裁，负责公司全球安全战略业务，他同期还是拉姆斯菲尔德防务政策委员会里的骨干成员，他的这个身份对公司的生意大有好处。伍尔西是高调的鹰派人物，他和切尼等人在1997年抛出过一份《美国新世纪计划》，鼓吹“美国可以按照自己的想法改造世界、统治世界”，可以“大胆地单方面使用美国强大的军事力量”“颠覆敌对政权”。[239]“9·11”事件之后，伍尔西主张对伊拉克动武。同时，他又很有商业头脑，很早就嗅到小布什发动“反恐战争”带来的商机，预测到政府和企业都将在这方面投入大量资金，于是成立了自己的帕拉丁资本集团，专门针对国土安全和反恐市场开展业务。[204, 240]

为了获取情报界的信息，博艾汉公司还开辟了一个渠道，这就是“情报及国家安全协会”（INSA）。这个协会的主要作用是打造一个承包商和政府官员可以私下聊天的场所，协会下设董事会、顾问委员会、执行委员会等，成员则来自博艾汉、洛马和诺格这样的私营公司，以及白宫科技政策办公室、国安局、国防情报局、国家地空情报局这样的政府部门，[241～243]简而言之，涵盖了美国情报圈的主要成员。博艾汉公司在这个协会里扮演了举足轻重的角色——时任公司资深副总裁的麦康奈尔曾主导了协会的重建，博艾汉还和洛马、诺格、BAE系统、波音、雷声等公司一道成为协会的顶级会员。[244]麦康奈尔担任国家情报总监后不久，就和协会一起举办了“国家情报总监行业日”活动，参加活动的协会成员有机会了解国家情报总监的战略规划以及优先资助的任务领域等情况。[204]要知道那些投入巨额游说资金的公司最多也就是得到这样的交流机会，协会让这样的交流变得轻而易举，而且经济实惠。

博艾汉公司与美国陆海空三军的关系也非比寻常。如果要排序的话，海军第一，有20个副总裁级别以上的公司高管曾是海军军官或者在海军中服务过。陆军第二，有17个；空军第三，12个。这跟公司与三军的合作时间的长短顺序正好一致，与海军合作有70多年、陆军60多年、空军20多年。可见合作时间越长，社交网络越有效。[233]三军如此，国防部也不例外，“旋转”到博艾汉公司的也大有人在。资深副总裁亨利·奥伯林（Henry Obering）曾经是国防部导弹防御局局长，现在的主要客户是空军航材司令部、空军航天司令部和国家航空航天局。[245]另一位资深副总裁史蒂夫·苏乐斯（Steve Soules）曾当过国防部联合C4ISR决策支持中心主任，现在负责提供面向国防部的高级情报分析服务。[233, 246]

除了重视上层路线，博艾汉公司对美国三军的“群众基础”也非常重视。他们号称，公司1/3的员工都曾有过军旅经历，[247]并且连续多年进入《GI　　Job》杂志最佳退役军人就业公司排行榜，成绩相当突出：2010年排名第14，2011年排名第1，2012年排名第4。[248]

有了如此深厚的资源，博艾汉公司成为联邦政府部门“人见人爱”的合作对象就一点儿也不奇怪了。但博艾汉公司并非孤例，国会下属的政府问责办公室（GAO）2008年做过一项调查，2435名国防部前官员“旋转”到了52家国防承包商那里工作，其中有65%的人不约而同地集中于7家情报承包商。这7家最受国防部官员欢迎的公司前面都提到了：科应、诺格、博艾汉、L-3通信、洛马、通用动力和雷声。有近1/3的国防部前官员从曾经工作过的部门那里拿到了合同，实现了“肥水不流外人田”。[249]

2002年前后，博艾汉公司得到了国防部“全面信息感知”（TIA）项目的部分合同，这个项目非常重要，后面还会专门讲到。[250]公司指派原陆军情报军官威廉·万斯里（William　Wansley）带领一个团队，为中情局国家保密处的战略规划和业务计划工作提供支持。而海军原情报军官伦兹带领着一个120人的团队，为国家侦察局提供支持。[250]就在斯诺登事件爆发前几个月，博艾汉公司还和其他11家承包商一起，赢得了国防情报局价值56亿美元的一单合同。接着，它又和另外几家公司一起，承包了海军情报部门价值10亿美元的项目。[250]

但像博艾汉这样的“旋转门”公司与情报和安全部门之间的合作并不一定很轻松，有时还会出现很大的问题。下面要讲的就是这样一件事情。

“国安局现代化计划”

2000年1月24日，周一，这是载入国安局史册的一个日子。

傍晚时分，海顿局长吃过晚饭正在看电视，突然电话响了。电话那边的人有点儿语无伦次。

“你说清楚点儿，发生了什么事？”

“整个系统宕机了。”[251]

这一回局长听清楚了。三天后，经过几个昼夜的抢修，瘫痪的系统终于恢复了大约25%的处理能力。海顿再一次接到电话，技术主管请求他授权彻底重新启动系统。到周五早晨，系统一点一点地重新恢复了知觉。[251]在后来的一档电视节目里，海顿对这周发生的事情用这样一句话进行了概括：国安局经历了一次脑死亡。[252]

从1999年3月海顿当上国安局局长的那一刻开始，他的心情就没有轻松过。欧盟发起了一场针对国安局秘密监听行动的调查活动，报上整天都是这些新闻。这项监听行动的代号叫作“梯队”。[252]更让新局长不安的是在国安局内部：五个分局各行其是，自己根本指挥不动；财务系统非常混乱，预算有问题，可就是不知道问题出在哪里；局里各式各样的委员会居然多达452个；给局长提供建议的高级政策委员会总是争论不休、无法达成共识；在总部竟然同时运行着68个不同的电子邮件系统；网络方面没有人可以掌握全面的情况，发生故障后连可以参考的布线图都找不到。[115, 251]

最要命的是新技术。越来越多的通信采用难以被监听的光纤传输以及难以破解的加密手段，监听范围的爆炸更是史无前例的：40年前全世界只有5000台计算机，没有传真机，也没有移动电话……到1999年，全球计算机数量超过4.2亿，其中大部分已联网，传真机大概有1400万部，移动电话4.68亿部，而且这些数字仍在持续增长。[114]众议院情报委员会发出警告，国安局“问题严重”：

信号情报面临着危机。自“二战”后的50年中，我们一直生活在信号

情报的光荣时代……以往，技术是国家安全局的朋友，但时间刚过去四五年，技术就已经变成它的敌人。[114]

新闻媒体上则是这样说的：“新技术造成的困难威胁着国安局，使它的‘大耳朵’越来越聋。”他们还说：“国安局在先进技术方面已经落伍，无法对付恐怖分子、黑客以及其他威胁。”[115]

支撑国安局“光荣时代”的有三大支柱：预算要多少有多少、技术上一家独大、主要敌人只有一个（苏联）。随着冷战结束，其中的两大支柱一夜之间就坍塌了：苏联解体了，随之而来的是“鸟兽尽，良弓藏”；在20世纪的最后10年，国安局的预算被削减了1/3，人员也裁减了1/3。[251]可这10年又是信息技术（特别是计算机技术和网络技术）裂变式发展的10年，整个世界发生了巨变。反观国安局，由于力量被削弱，只能依赖陈旧的技术系统，面对新技术浪潮的到来，它根本没有做好准备。

海顿下令成立两个工作组，检查国安局这部“老爷车”的毛病到底出在哪里。内部工作组由局里的19位中层管理人员组成，外部工作组聘请了5位外界管理专家。调查结果触目惊心：国安局越来越落后，正逐步衰败，无法面对全球网络崛起带来的各种问题，管理层根本不能适应势在必行的改革。员工分成三派，25%强烈支持改革、25%坚决反对，剩下的50%摇摆不定。[114, 251]海顿别无选择，只能大刀阔斧地大干一场。1999年11月，海顿推出了一个“百日变革”计划，准备用三个多月的时间把许许多多改革举措落实到位。[114]2000年年初的这次系统崩溃更加坚定了他推行改革的决心，也为他推进改革增加了一个现实的反例。局长自己是信号情报的门外汉，他非常担心其他精通信号情报的局领导不愿意改变现状[251]，这次宕机事件对新局长推行变革来说反而是件好事。

海顿把加快国安局的现代化进程列为这次改革的重头戏。在“国安局现代化计划”之下，他部署了两个重点项目，一个叫“创始人”，另一个叫“开拓者”。[253]这两个名字响亮又给力，从一个侧面反映了局长此时此刻的劲头。他的策略也很简单，只有一个字——“买”。对此海顿曾经说过这样一段话：

我们要从美国工业界那里购买系统，而不是自己开发系统。我们并不需要拥有美国最顶尖的聪慧之人和发明创造，我们只需要找国防承包

商，让他们想办法，帮助我们适应数字时代的要求。[254]

“创始人”项目的主要任务只有一项：实现国安局内部日常使用的通信系统等基础设施的更新换代[255]，并且把这些系统和设施的运维业务完全外包给私营公司。[256]博艾汉公司以顾问身份参与了这个项目。[257]项目最终确定的主承包商是计科公司（计算机科学公司）和隶属于诺格的罗技康公司，和他们竞标这份合同的还有两个团队，一个是科应和洛马等公司组成的团队，另一个是雷声和OAO等公司组成的团队。竞标过程前前后后用了两年时间，2001年正式签订合同，价值20亿美元。[258]项目正式启动之日正是1000多个国安局雇员变成私营企业雇员之时——继续裁员也是海顿必须完成的一项“硬任务”。局长想出了一个一举两得的“妙招”：公司与国安局签合同时必须接受一个附加条件，即接收被裁掉的国安局员工。海顿的如意算盘是：在推进国安局现代化的同时，也完成了裁员任务。当时的人事主管回忆说：“这些人周五离开的时候还是国安局雇员，下周一回来已经变成计科公司的雇员。”[255]

参与“创始人”项目的公司有40多家，为了更好地协调力量，他们组成了一个“老鹰联盟”。不过项目的进展并不顺利，最终竟变成了一个时间不断后延、投资不断追加的钓鱼工程，开销一路涨到50亿美元。[255]效果如何呢？有些分析人员和管理人员说他们的效率降低了一半，原来摁几次键就完成的事情，现在需要很多步骤；还有人报告说，他们的机器有时候在没有任何提示的情况下就被锁住了；翻译人员则抱怨，他们使用“创始人”之后，完成的翻译工作量明显下降了。[259]

国安局总监察官在2003年9月的一份报告中写道：“创始人”合同管理的诸多“关键要素”缺失，没有合同管理计划，也没有质量控制机制，等等。报告还披露，数百万美元的开支不知去向。[259]在联邦政府看来，“创始人”的这些问题似乎并不算严重：项目按期结束后，国安局和这些公司又续签了三年合同。[255, 258]相比之下，“开拓者”就要糟糕得多了，它几乎被一致认为是一场灾难。

“系统错误”

“开拓者”项目的主要任务涉及国安局的核心业务——数据分析和处理[252]，这个项目可以被看作驱动国安局进入数字时代的引擎。

早在20世纪90年代，国安局高层就已经认识到，他们能够通过各种途径搜集到大量数据，却没有足够的能力分析和处理这些数据，结果就是“数据过载”。[260]当时的局领导责成“信号情报自动化研究中心”（SARC）解决这个问题。这个研究中心是国安局内部的“臭鼬工厂”，更直接一点儿说，就是国安局下属的一个技术研发单位。他们提出，需要建设一个处理和分析海量通信数据的信息系统，他们把这个系统叫作“细线”。[260]

威廉·宾尼（William Binney）是研究中心的技术主管，也是密码和数学方面的专家，被认为是局里最厉害的分析专家。他首先对需要处理的数据总量进行了一番粗略估计：全世界的电话总量约为25亿部、IP地址大约15亿个，每分钟全球传输的信息总量有20太字节。[260]面对如此大量的数据，工作人员只能利用信息来源和关键词对数据进行简单地筛选，挑选有用数据、丢掉无用数据。熟悉这些工具的人打了一个比喻，这就像根据信封上的信息来决定是保留还是丢弃一封邮件。大约95%收集到的信息被直接过滤掉了，只有约5%的信息被转交给相应部门做进一步的处理和分析。[252]

按照宾尼的设计，“细线”项目能够发现商务交易、旅行记录、网络搜索、位置信息等各种数据中隐藏的关联，这就叫作“数据挖掘”，利用这种方式，分析人员可以得到锁定那些“坏蛋”的有用信息。他说：

我想绘制全球关系图。有人说，你实现不了，因为其中有无限种可能。但是，在某个给定时刻，就连宇宙中原子的数量也是有限的，尽管这个数字会非常巨大。[260]

宾尼带领着一个20多人的团队，开始了系统设计工作。[260]他们开发出了4个技术先进的工具，部署在不同节点上，对搜集到的电话数据和电子邮件数据进行分类。[261]在“星风”行动中，主要搜集和处理的就是这两种通信数据。

宾尼他们设计的工具颠覆了国安局过去的数据处理模式。过去，中心节点之外的其他节点只负责搜集数据，所有数据都传输到中心节点去处理和分析。而宾尼团队的方案是，分散在不同节点上的工具都进行计算，把通信人之间的关联挖掘出来，把可疑的通信记录找出来，只把有用的数据传到中心节点，其他数据则丢弃。这样，不仅降低了数据传输压力，也降低了中心节点数据过载的危险。对此，宾尼颇为得意："它的美妙之处在于开放性，因此它是可以不断扩展的。"[260]

在1998年的试验过程中，"细线"项目成绩斐然，各项任务得分都很高，在性能方面远远优于当时使用的系统。[261]到2000年，依托高速光纤网络，"细线"项目已经能够实时绘制出社交网络关系图。[260]国防部总监察官在2004年12月发布的报告里指出，2001年的"细线"所具有的性能甚至优于2004年国安局部署的新系统。[261]但是，该项目的命运在悄悄地发生逆转。为了保护美国人的通信隐私，宾尼他们还设计了专门的工具，对涉及美国人的通信数据进行加密处理。可国安局的律师们认为，"细线"项目对隐私的保护远远不够，还有些人对这些工具能否支撑大规模的数据心存疑虑。[260]

据说，海顿局长是听从了法务长的意见，舍弃了存在隐私保护缺陷的"细线"项目。但也有人认为主要原因并非如此，局长想要的是能一次性解决各种棘手问题、塑造国安局未来的"高端"工程，像"细线"这样的小动作、解决局部问题的项目明显不合局长的心意。[260]这种看法不无道理。说这话的人名叫马修·艾德（Matthew Aid），他对国安局颇有研究，曾写过一本有关国安局的书，书名叫作"秘密哨兵"（*The Secret Sentry: The Untold History of the National Security Agency*）。

海顿抛开"细线"，"钦点"了一个崭新的秘密项目，这就是"开拓者"。从一开始，这个项目就被理想化和复杂化了。"开拓者"计划最初考虑的优先需求有1000多条，但这个计划先后由三个不同的部门来牵头，他们又分别根据自己的理解把更多的要求加了进去。这三个部门，第一个是新成立的改革办公室，可它只存在了一年就被撤销了；第二个是信号情报分局，那里的情报分析人员很多；第三个是信息技术分局，主要负责技术系统建设。这些部门都认为这个项目是自身发展的一个难得机遇，不约而同把自己想做的事情放进局长"钦点"的项目里，这样就不用担心有预算被削减的危险。每次更换牵头部门，"开拓者"计划都会进行一次大"整容"。[252]

“9·11”事件发生后，美国人在其情报和安全部门开展了大范围的调查活动，全面查找问题。他们发现，过去三年里他们一共搜集了30多条有用线索，可惜它们都躺在国安局的数据库里“睡大觉”。[252]而酝酿多日的“开拓者”到这个时候还没有“出窝”。有人批评说，如果部署了“细线”项目开发的工具，很可能提前发现并阻止恐怖袭击的发生。[260, 261]

直到2002年，国安局才确定了哪四家公司将参与“开拓者”项目。主承包商是科应公司，这个名字在前面曾经被提到过多次。被小布什委以重任，负责调查伊拉克大规模杀伤性武器的戴维·凯在这家公司里担任副总裁多年。剩下的三家公司则会作为科应公司的助手，它们是博艾汉、波音和计科公司。[262]

事后有人批评科应公司，面对国安局提出的种种不现实的要求，公司没有说一个“不”字。[252]科应公司如果不是“无知”，那就一定是“无畏”。因为海顿局长还“钦点”了项目的监管人，此人名叫威廉·布莱克（William Black, Jr.），当时的身份是国安局常务副局长。他在国安局工作了近40年，1997年从信息战主任特别助理的位置上“退休”[114]，“旋转”到了科应公司，当上了公司的副总裁（也有人说是公司的助理副总裁[263]）。海顿上台后不久，就把他召回了国安局，而且让他当上了常务副局长。邓普西副局长发表过一番借鉴公司经验可以更好地当好政府高官的高论，可惜布莱克的公司经验并没有帮助他管理好“开拓者”项目，这也从某个侧面说明，邓普西的那番高论只是她的想象。

相比于博艾汉公司，科应公司更加隐蔽低调。所以，当媒体披露由这家公司担纲“开拓者”项目的时候，用了“几乎不为人所知”来形容他们。实际上呢？这家公司在旋转门公司的行列里绝非等闲之辈。它的董事会名单拿出来也是很有派头的，国防部前部长梅尔文·莱尔德（Melvin Laird）和威廉·佩里（William Perry）、前中央情报总监约翰·多伊奇（John Deutch）和罗伯特·盖茨（Robert Gates）、国安局前局长博比·印曼（Bobby Inman）都曾出现在这个名单上。[263]

除了布莱克副局长跟科应公司关系密切，还有一些事情让人匪夷所思。项目进行到中途，国安局的两位高官哈尔·史密斯（Hal Smith）和山姆·魏斯那（Sam Visner）竟然“下海”去了科应公司，而史密斯到科应公司之后，除了继续进行“开拓者”项目，同时还兼职做联调局的一个项

目。可惜，联调局的这个项目也是结果惨淡，在扔进去1.7亿美元后不声不响地中止了。[263]

据爆料人称，由于使用了蹩脚的数据分类工具，“开拓者”的分析性能受到拖累，导致系统产生大量的错误分析结论，许多人错误地被怀疑和调查。更由于取消了隐私保护机制，分析人员无须申请法庭调查令就可以开展调查，数据记录实际上处于被滥用的状态。[261]

国安局总监察官在2003年的报告中指出：国安局未能对“开拓者”的进度和结果进行充分和有效的监督，也未能掌控全部的经费流向。而2004年国防部总监察官报告披露，“开拓者”项目并没有研发合同要求的系统，也不可能研发出这样的系统。这份报告还建议对国安局的整个财务系统和采办系统进行调查。“细线”看上去比“开拓者”更接地气，也可以被更快地部署。[252]但是，在这场和“开拓者”的竞争中，“细线”明显处于下风，原因并非技不如人，而是身后无人。就在国防部的这份报告出台后不久，国安局就对“开拓者”项目进行了调整，将牵头公司改为IBM公司。考虑到反恐战争的形势，国会并没有砍掉任何一个与反恐有关的项目，包括“开拓者”这样问题严重的项目，所以“开拓者”仍然“活”着，但只能“蹒跚前行”。[252]国安局因为这个项目损失巨大，他们自行签订大单合同的权力被国会剥夺了。从此以后，所有国安局数额较大的合同都必须先经过国防部的批准才能生效。[259]

到2005年4月，海顿在国会听证会上不得不承认这个项目存在“拖”和“涨”的问题：项目进度落后，合同经费达5亿美元，还超支了一两亿甚至更多。但他没好意思提到“降”的问题——开发出来的东西其实不太好用，估计是实在说不出口，他便只是含含糊糊地说这个项目“比所有人预期的都难得多”，以此给自己预备一个台阶。[252]但这一切被严格保密，外人并不知道。

一朝天子一朝臣。随着海顿局长的离任，国安局的历史翻开了新的一页。新任局长名叫基思·亚历山大（Keith Alexander）。上任伊始，亚历山大局长就不得不面对前任局长留下的大窟窿，但他起初考虑的还只是对“开拓者”进行修修补补，而不是彻底抛弃。2006年1月29日，《巴尔的摩太阳报》登出了一篇题为“系统错误”的文章，揭开了“开拓者”的盖子，也给它敲响了丧钟。[252]文章一登出来，亚历山大局长就有了一个很充足的理由，让“开拓者”彻底下马。一旦实现，海顿局长留下的大包袱就可以“一风吹”了。对新局长而言，这个机会实在难得。他没有

一丝一毫的犹豫：一边果断终止了“开拓者”，一边马上启动了属于他自己的项目，代号“动荡”。“动荡”这个名字看上去有点儿不吉利，项目后来的进展也真的是磕磕碰碰、跌跌撞撞，也算是一语成谶吧！宾尼就把“开拓者”称作“1号五年计划”，把“动荡”称作“2号五年计划”。[264]

“开拓者”终于下马了，截至此时，投入的总经费已远远超出了预期，甚至远远超过了海顿所说的5亿美元，达到了12亿美元。但项目的最终结果非常惨淡，提出的关键目标一个也没能实现，成为“美国情报界有史以来最大的一个‘打水漂工程’”。[252]

海顿是国安局历史上曝光度最高的局长之一，他经常在媒体上抛头露面，甚至同意接受长期研究国安局的詹姆斯·班福德（James Banford）对他进行专访。班福德1982年写作的《迷宫》是世界上第一本专门讲述美国国安局的书。相比之下，他2001年出版的《秘密的肌体》更为轰动，这本书2003年在中国翻译出版，书名改为“秘密机构：美国国家安全局揭秘”，可惜书中有一些翻译不够准确的地方。2008年，班福德出版了其第三本有关国安局的作品《影子工厂》，这本书成为《纽约时报》年度畅销书，被《华盛顿邮报》评为“年度最佳图书”。不过这本《影子工厂》读起来过于琐碎，不如《秘密的肌体》那么“货真价实”。

海顿的高调给他和国安局带来了不少“麻烦”，他经常需要向国会和大众解释问题、回答质疑。可能是从前任身上汲取了“教训”，亚历山大明显加强了保密工作。关于“动荡”这个项目的情况，被披露出来的东西很少，甚至有哪些公司参与项目建设都成为秘密，至今没有公开。

目前已知的一件事是，局长对国会使用了障眼法：化整为零、躲避监督，使得这个已经实际存在了若干年的项目，在国安局的年度预算上却找不到，这令国会议员们非常气愤。被披露出来的另一件事情是，计划含糊不清、研发进度滞后等问题困扰着这个项目，亚历山大对它也逐渐失去耐心。在项目管理方面，“动荡”开始出现当年“开拓者”出现过的种种问题。好在项目最后还是形成了一批可用的成果。在这个项目里包含了9个核心组件，媒体上点出了其中三个的代号：“混乱”“监护”和“流量贼”。[265]请记住这三个代号，有关它们的更为具体的情况就要靠斯诺登来揭秘了。

至于海顿局长，尽管“开拓者”和“创始人”这两个项目让他蒙羞，但

他在国安局雷厉风行地进行改革，给国会留下了深刻印象，他们想方设法延长了他的任期。通常情况下，国安局局长的任期只有三年，他却在国安局局长的位置上待了6年。[114]2005年海顿离开国安局，升任美国国家情报第一副总监，一年后又被提拔为新一任的中情局局长。三年后，刚从局长位置上退下来的海顿先生转身加入了某家公司的“赛博顾问委员会”。能猜出来是哪家公司吗？是“创始人”项目的主承包商计科公司。这也算是给“旋转门”增加了一个鲜活的实例。[266]

鱼龙混杂

“旋转门”的故事还有很多，涉及的公司也远不只凯雷、博艾汉、计科、科应，以及上面提到的其他公司。在美国，“旋转门”有它存在的合理性和必然性。简单地说，其根源是美国的政治体制，想要消除“旋转门”根本不可能。以美国行政部门为例，进入这些部门工作，有两种渠道：一是靠“选”，即招聘、选拔；二是靠“点”，就是任命、点招。美国政府高官都是靠第二种渠道进入行政部门工作的。例如查尔斯·哈格尔（Charles Hagel），从参议院退休后，他被奥巴马提名、任命，成为美国第24任国防部长。离职或者退休后，这些政府官员或者雇员都面临养家糊口的问题，要想维持品质较高的生活，就更加不易，所以“转”到公司发挥余热，在美国人看来是很正常的事情。问题是，怎样防止他们以权谋私。而这在美国法律上也是有说法的。

《美国政府道德法》规定，行政部门的高级官员在离职或退休后一年内不得受雇于任何公司或机构，对其原供职的政府部门开展游说活动。1989年，国会又通过了《政府道德 改革法》，细化和修订了监管措施，把立法部门和司法部门也纳入了监管范围。但是，高官身边少不了法律顾问的影子，这些法律高手总能找到办法，绕过法律，让这些规定形同虚设。比如，法律规定，公职人员从高级别职位上退休后，不得代表其他个人、企业或机构为任何事宜而联络或出现在其原就职部门以寻求任何官方行动，“冷冻期”为一年。与此同理，更高职务的公职人员离职后的“冷冻期”为两年，所受限制更为严格，包括不得与任何政府部门或机构达到一定级别的高级官员接触。[267]针对“冷冻期”，只要找到可靠的中间人作为退下来的高官的代表，让这个中间人在政府部门游走，就可以完成看上去不可能完成的任务。

“旋转门”不仅普遍存在，而且其内部也早已盘根错节。那些明显带有“旋转门”色彩的公司看起来已经结成“利益共同体”，其中一种模式就是建立类似于“情报及国家安全协会”这样的比较正式、比较固定的组织。另一种模式就是临时结盟。联邦政府的大项目往往会分给几家公司而不是由一家公司独立承担——美国政府似乎也深谙“不能把所有鸡蛋都放在同一个篮子里”的道理，于是，共同承担项目的几家公司自发联合起来，建立“攻守同盟”，同进同退、有福同享、有难同当。比如“开拓

者”，再比如“创始人”，都是如此。

也有人公开替“旋转门”辩护。他说，旋转门也有它好的一面，如果没有离任的高官指引，私营公司在政府采办的道路上就会举步维艰。此言一出，这个人立刻引起无数人的关注。此人名叫雅克·甘斯勒（Jacques Gansler），他自身的经历就是旋转门的典型代表。他先是在雷声等防务公司沉浸多年，于1972年进入国防部，先后担任负责采办的助理部长帮办，以及负责电子领域的国防研究开发署副主任。1977年，他转到塔斯克公司，一干就是20年，一直做到公司的执行副总裁和董事。塔斯克公司是美国信息技术应用领域的重要防务承包商。1997年甘斯勒回到国防部，担任负责采办、技术和后勤的次长。4年后，他转出国防部，进入马里兰大学，成为大学教授，负责马里兰大学公共政策和私营企业中心的建设和管理，同时担任iRobot和塔斯克等多家公司的董事。这样一个人替“旋转门”辩白，不免让人觉得有些越抹越黑。[263, 268]

博艾汉公司并不是行事鲁莽、只知道挣钱的“土豪”公司，它曾先后创造了许多给商业管理带来巨大影响的概念，首先就是“管理咨询”，这个词后来成为一个行业的标签。然后是20世纪40年代创立的“人力资本”、50年代的“产品生命周期”、80年代的“供应链管理”、90年代的“灵巧定制”，以及最近的“组织基因”。[269]除此之外，还有“PERT网络分析法”、“无中心的公司”等。[270]如此看来，在“旋转门”公司里，博艾汉真还算是很有学术风范的。

只要反恐这面绝佳的大旗一天不倒、反恐战争一天不结束，这些“旋转门”公司就可以继续从联邦政府手里得到海量的合同，和某些官员实现“共赢”。要充分满足联邦政府的任务需求，公司似乎只有一个办法：大量招聘社会人员。

说到情报部门的任务需求，人们往往会产生一个错误的印象，以为这些工作岗位都是“高端洋气”的，甚至带有一些执行特工任务式的神秘色彩，其实不然。国家情报总监办公室把需要外包的工作分为三类。

第一类叫作商业服务承包，这类工作涉密程度最低，工作内容不需要什么技能，工作层次甚至有点儿低微，例如情报单位的园林绿化、卫生保洁、安全门卫、邮件收发和食品餐饮。但是，即使是在情报安全单位做一个保洁员，也需要获得一定的安全许可——翻检垃圾桶都有可能

接触涉密信息。别小看了安全许可，因为大多数获得安全许可的人的学历并不低，让他们去打扫卫生明显是人才浪费，所以这类岗位有时候还真的很难招到人，想去做的人不符合要求、符合要求的人往往又不愿意去做。[174]

第二类叫作设施设备承包，这类工作为情报单位提供从卫星到计算机等设施设备服务，计科和L-3通信公司专注于经营这一级别的业务。博艾汉虽然也涉足这类工作，但其重心在第三类工作上。

第三类叫作核心人员承包，涉及关键任务的完成。例如，参与拟定击溃伊斯兰北非“基地”组织的策略，或者进行软件设计，或者给高级官员充当文字秘书、为他们撰写讲稿。[174]连《总统每日简报》这样的重要情报产品，很大一部分竟也是由博艾汉、科应、凯西等公司的聘用人员完成的。[271]

其实，除了这三类工作，还有一类外包业务工作，可以称之为基础业务承包，其特点是需要一些专门技能，例如翻译、安全许可背景调查等都属于这一类。[174]其中，因为有大量海外通信、文件翻译和电子语音监听任务需要完成，翻译人员也颇为紧俏，2010年有56家公司在提供翻译服务。[232]

这四类人员加在一起，形成一支浩浩荡荡的聘用人员大军。以中情局为例，2010年局里有1/3的工作岗位属于聘用人员，他们来自114家公司。国安局聘用的人员则更为分散，涉及大大小小484家公司。[232]据美国国家情报总监办公室统计，2008年，仅“国家情报计划”就聘用了三四万名私企人员，人员中的27%从事情报搜集和处理工作，19%从事情报分析和报告拟制工作，22%坚守信息技术岗位，还有19%做的是辅助性或者日常管理类工作。也就是说，这三四万私企人员中的87%，都在比较高级别的岗位上工作。这些人当中，73%在各个情报单位的办公区里工作，其余27%跑外勤，其中一些还被派驻伊拉克或者阿富汗。[249]

这里需要稍微解释一下“国家情报计划”。美国政府的情报预算分为两个部分，一个就是国家情报计划，另一个是军事情报计划。顾名思义，军事情报计划主要支持美国军方的情报行动，国家情报计划则主要支持国家层面的情报活动，但其实很多经费仍然投给了国防部。不要忘了，国安局隶属于国防部，它的主要经费来自国家情报计划。

由于社会上拥有绝密安全许可的人员特别紧俏，因此，俗称“人力资源商店”的专向猎头公司应运而生，介绍一个拥有绝密安全许可的人员的中介费高达5万美元。在奇货可居的情况之下，2010年这样的猎头公司超过了300家。[232]

威廉·高登（William Golden）现在是IntelligenceCareers.com网站的负责人，这个网站就是一家猎头公司。在他的网站上就发布过博艾汉和其他公司的“情报搜集主管”招聘启事。情报搜集主管处于情报单位的高层，可以决定哪些情报被采用、如何被采用，还能决定情报的去向。高登说，这些私营公司的雇员有思路、有方向、有办法，除了不能使用经费、批准经费，不能招聘或者解聘政府雇员之外，他们可以做其他所有事情，几乎和政府雇员一样。[174]关于这个高登，这里还想多说一句。他曾在陆军服役22年，其中有10年是在国安局设在日本三泽基地的侦听站度过的，[272]曾经有人认为这个侦听站是斯诺登在日本的工作单位。

但俗话说“林子大了，什么鸟都有”，以博艾汉公司2.4万人的规模来看，其中个别人员出现一些问题在所难免。

2008年公司曾经聘用过一个叫斯科特·本奈特（Scott Bennett）的人，他被判缓刑三年后才不过几个月就得到了最高密级的许可，并且顺利进入博艾汉公司工作。[177]正应了另一句俗话，叫作“萝卜快了不洗泥”。这位老兄后来也没消停，他又因为欺诈、非法持有枪支等罪名被判刑入狱，媒体报道他的时候还捎带着点了“博艾汉”的名字。说起他这次的事情有点儿可笑。据报道，他身穿制服，跑到美国麦克迪尔空军基地住房办公室，谎称自己是特种作战司令部领导的助手，要办公室马上给将军弄一套房子。办公室要他拿出证明等材料，却最终被他成功应付了过去。就这样他居然在基地里蒙混了好几个月，直到一次突击检查时才暴露。但由于本奈特此时已经离开博艾汉公司，公司各方面都没有因为他的这点儿小事受到任何影响，所以，他当年“混入”博艾汉的过程也没有引起公司的足够重视。[273]

相比于下面这件事情，“本奈特事件”就显得微不足道了。2012年2月，媒体突然发布了一条消息：美国空军圣安东尼奥办事处停业整顿，这家办事处的员工全都来自博艾汉公司。大约一年前，这家办事处招聘了退役空军中校乔斯利托·孟尼塞斯（Joselito Meneses）。进公司的时候，中校随身携带了一份“见面礼”：一块载有敏感信息的硬盘，这些信

息有助于博艾汉公司在随后的一次合同竞标中获得优势。办事处相关负责人不仅没有询问敏感信息的来源是否正当，甚至还让中校本人直接参与了这次竞标活动。但这些情况没有逃过群众“雪亮的眼睛”，有人向博艾汉公司总部举报。公司很快查明：情况的确属实，于是果断采取措施，解聘孟尼塞斯中校，并且退出有关的合同竞标。[274]他们以为这样就算解决了，只是非正式地向空军说明了一下情况；但空军方面认为公司的态度不够“端正”，如果不趁着这件事狠狠纠治一下，将来类似的事情还会发生，并且有可能成为一种常态。这才有了暂时关闭办事处的这一幕，此举也的确让博艾汉公司真正重视起来。在办事处关门整顿的两个月期间，公司专门聘请了第三方公司来改进思想、整顿工作、强化内部调查机制，未来三年还将持续向空军报告有关情况，并且将孟尼塞斯中校的直接上级也一并开除。此外，公司还付给空军6.5万美元“补偿款”。至此，空军才同意重新开放办事处。[177, 275]事情总算告一段落，影响不算大，也不算小。

但“孟尼塞斯事件”仅仅过去一年，一个出身平常、学历也不耀眼的年轻人在进进出出“旋转门”公司的滚滚人潮中，“混入”了博艾汉公司。更准确地说，这位年轻人是带着明确的目的“潜入”博艾汉公司的。[276]公司对他的“险恶”动机根本没有察觉，更没有预想到他蕴含的能量是如此之大。

这一次，博艾汉公司终于名声大噪。这个年轻人就是爱德华·斯诺登。

第四回 “80后”斯诺登

年轻人斯诺登的全名是爱德华·约瑟夫·斯诺登，生于1983年6月21日。按照中国人的习俗，他属猪；按照西方的习惯，他所属的星座是双子座；按照他的说法，自己生逢夏至，那是1983年最长的一个白天；[277]而按照时下流行的说法，他是一个“80后”。据说这个孩子思想深刻、口齿伶俐。他给国安局捅下了天大的娄子之后，局里对他进行抹黑也可以理解，无非是从历史上、在品德上把他拉入黑名单，说他在国安局入职考试中作弊，说由于担心他工作用过的计算机可能被他安装的恶意软件感染，只能销毁，等等。[278]

如果智力测试准确的话，斯诺登算得上聪明过人，他两次不同的智力测试结果都超过了145分。[15]在过去的同事眼里，斯诺登是“天才中的天才”，这种形象和“官方”版本大有不同。到夏威夷工作之前，斯诺登开发的一个备份系统被广泛应用于密码破解行动，这让他的上级主管印象深刻。他是作为网络安全专家来到夏威夷的，根据合同要求，他的岗位是微软Sharepoint系统管理员。但由于他的能力出众，上司考虑让他负责建立一个新的Web前端系统，尽管这可能超出了他的工作范围。斯诺登工作积极主动，不时发现并报告单位软件中存在的漏洞，其中许多漏洞从未打过补丁。[278]

斯诺登并不愿意过多谈论他的个人情况。他非常不愿意把自己的家庭牵扯进来，也不愿意大家把他做出的这一“惊天动地”的事情搁置不谈，而把关注的焦点放在他这个人身上。他说：

我是一个工程师，不是一个政客。我不想登上舞台。我很害怕那些“名嘴”（借用我来）分散公众的注意力，（从我身上）找到借口，危害并对一次非常重要的行动泼污水，甚至使它非法化。[15]

他的这种担心并非没有道理。但是，掀起如此巨大波澜的人物怎么可能不登上舞台？公众又怎么可能不对他刨根问底、评头论足？

这是不以他的意志为转移的。

安全专家

斯诺登不是独生子，他上面还有一个姐姐。斯诺登9岁时随父母从北卡罗来纳州的伊丽莎白城搬到了马里兰州的克罗夫顿，该地距离国安局总部不过15英里（约24公里）。[279]这是一个安静的小镇，安静到有点儿奇怪，即使是上午的咖啡时间，镇上的星巴克咖啡店也没什么动静。当地人很少在办公室以外的地方聊天。这里的居民多半是国安局的职员，以及为国安局工作的私营公司雇员。斯诺登在童年和少年时期表现得很平凡，并不出众，童子军同伴对他几乎没什么印象。[280]当同龄人或者坐在电视前几个小时不挪窝，或者在户外蹦蹦跳跳不到天黑不回家的时候，他却迷上了看书，而他最爱看的竟然是希腊神话。[15]

害羞的斯诺登并不能被归入品学兼优的“好孩子”的行列。升入中学之后，他一如既往地默默无闻。面对记者的追问，他的几个同学左思右想，竟没回想起关于他的任何一件事情，更不用说他的老师和校长了。只有一个男生，是他初中和高中的同学，还能记得他当时着迷于奇幻游戏、格斗游戏。[280]十年级的时候（相当于中国学制的高一），斯诺登因病辍学，后来通过考试拿到GED证书，也就是美国的普通高中同等学力证书。美国的教育体制实在让人惊奇：连高中都有“同等学力”！

接下来，他在安娜兰多社区学院学习，有关材料说他的专业是计算机，[281]可学校方面说他在那里并没有学习任何与计算机和网络相关的课程[282]。

国安局非常重视人才储备问题，他们有比较具体的落实措施：通过“国家信息保障教育训练计划”和国土安全部联手建立了一批“卓越学术中心”，也就是培训基地。斯诺登曾经就读的安娜兰多社区学院就是其中一个，不过由于是“学院”，它只有资格承担两年的教育计划。[283]斯诺登断断续续在这个社区学院里学习了两次，一次是1999~2001年，另一次是2004～2005年，但他既没有选修任何“与赛博有关的课程”，也没有学习获得国安局认可的“信息系统安全”课程，两进两出却没有获得任何学位。[282，284]按照美国陆军的记录，2002年，斯诺登进入卡斯顿维尔社区学院学习，可学校发言人说该校从1998年起就更名为巴尔的摩县社区学院了，那里根本找不到斯诺登的学籍记录。[282]这所学校也是

国安局的“卓越学术中心”之一。

2002年2月到5月，斯诺登在一家营利性的培训机构学习Windows系统工程的课程，这家机构名叫“先进职业技术”，借“约翰·霍普金斯大学计算机职业学院”的名义招生。关于这个名义，大学和培训机构双方都动了点儿脑筋。从英文名上看，这家机构与大学之间只有位置关系，没有隶属关系。换句话说，约翰·霍普金斯大学对培训机构的教学内容和教学质量没有什么信心，也不承担任何责任。培训机构这么做，多半属于“拉大旗，作虎皮”、玩个障眼法，欺骗不明就里的学生，而大学之所以同意对方使用自己的名字，估计也不是平白无故的。但这家机构在2009年结束了与约翰·霍普金斯大学的合作关系，并且在2012年彻底关闭。[282]

除了到学校“学习”，斯诺登还一直在动漫公司RYUHANA PRESS做编辑兼打杂。此时的斯诺登和许多同龄人一样，酷爱日本动漫和游戏。在公司网站上他贴出了自己卡通风格的名片，那形象和他本人的照片还真有几分神似。他如实填写了自己的出生年月，却谎称自己37岁，有两个儿子，一个11岁，叫“Lashawnda”，另一个12岁，叫“Tamiqua”。[285]

他在自己的简历网页上写道：

我的表现傲慢而残忍，因为我小时候得到的温暖太少，还因为公共教育系统把它肮脏的、长满大钉子的后脊梁甩给了我。[277]

这家小公司就位于国安局米德堡总部的隔壁，它的主要投资人是一帮大“孩子”。2004年，他们去加州上大学，顺便就关闭了这家公司，同时跑到学校附近另外开办了一家公司。[277]

2002年，斯诺登的家里发生了一件大事：他的父母离婚了。他和母亲搬到了埃里克特城附近居住。“80后”斯诺登自称信奉佛教，清心寡欲，很少出门。[286]面对自己并不光鲜的教育履历，他曾在网上发出这样的感慨：

伟大的人物不需要借助大学文凭使自己更可信：他们想要的东西、能静静照亮他们成功之路的东西，他们总能得到。[287]

他还说：

首先，学位的事情是不可靠的，至少在美国是这样。如果你真的有10年扎实的IT工作经历……你就能找到一份非常好的IT工作……我没有学位，甚至没有中学毕业证，但我赚的钱比他们给你的钱要多，虽然我只有6年工作经验。“闯进去”很难，但你一旦获得“真正”的位置，你就成功了。[288]

从这段话来看，斯诺登对学位颇为不屑，实际上却未必如此。他从2011年开始攻读利物浦大学的网络教育硕士研究生课程，虽然还没有得到学位[282]，但他已经忍不住在自己的求职简历里写上了这么一句：“预计”将于2013年的某个时候获得该校计算机安全专业硕士学位。[289]

2004年四五月间，第一次费卢杰战役打响。斯诺登突发奇想，打算到伊拉克前线大干一场，冲动之下他报名参军。按照美国政府的宣传，正在进行的伊拉克战争是一场解放被压迫民众的行动。“我愿意尽我所能。”[15]他是这样说的，也是这样做的。可是他的选择非同寻常：在没有任何从军经历的情况下，直接报名参加陆军特种部队。虽说他的考试成绩不错，[15]不过想要成为一名真正的特种兵，新征入伍的士兵还要经过三关：第一关是8～10周的基本训练，第二关是高级训练，第三关是考核筛选。斯诺登很快就因为自己的鲁莽选择付出了惨痛代价：几个月后他在训练中发生事故，双腿骨折，退役的时候他连基本训练都还没有完成。[282, 290]当时是2004年9月。这番折腾之后，他第二次走进了安娜兰多社区学院的课堂。

回过头来看他在训练中负伤这件事，其实很容易理解。试想，一个酷爱电脑游戏、一天到晚待在屋里的“宅男”，身体单薄，也未必动作灵巧，在特种兵训练场上很可能出现失误甚至受伤。毕竟，要想在现实世界里得到令人佩服的功夫和身手，可比在虚拟世界中靠键盘鼠标“修行”困难得多。

斯诺登曾经告诉别人，自己运用编程知识，只需摁下一个“x”键，就可以代替一组复杂刁钻的按键，在游戏里完成极其复杂的“必杀技”：两记重拳组合，外加风神腿，躲过高处的袭击。他可以一手拿着啤酒，只用另一只手打游戏，好不惬意。[291]他非常喜欢动漫游戏“铁拳”，也练就了一身高超的“武艺”，在2002年美国动漫大会上他的一番表现吸引了许多同好的目光，大出风头。[277]斯诺登对游戏的痴迷，并没有随着时间推移而消退。多年以后，他仍然会冷不丁地在网上发出这样的帖

子：

今天早上，我醒来的时候（为我的游戏角色）想到了一个新的名字，就叫狼王，“惊倒狐”狼王。[292]

在邻居的印象里，这是一个一天到晚坐在笔记本电脑前鼓捣的小伙子，每天都要弄到很晚。他自己是这样回忆的：

我感兴趣的一件事情是，如何把复杂的系统组装起来。所以，我把它们拆了又装、装了又拆，不分昼夜。我学会了一些东西，这些东西一次又一次地让我的生活受益。[279]

最早曝光斯诺登情况的英国《卫报》说，2005年斯诺登进入国安局设在马里兰大学的一家隐蔽单位当“保安”，这是他人生当中的第一份工作。[293]如果没有发生后来的故事，斯诺登这段当保安的经历很可能会让人感慨感动。

这家藏匿于马里兰大学校园内部的国安局单位具体发挥什么职能，按道理说，这所大学里的学生应该知道大体情况，但他们显然不清楚斯诺登究竟在哪家单位待过，只知道马里兰大学的物理科学实验室、通信科学实验室等单位与国安局关系紧密。[295]这些是大学生们在自己主办的一份校内报纸上说过的话。

学校很快通过发言人给出了一个官方说法：2005年，斯诺登在该校的语言高级研究中心做过不到一年的“安全专家”。这家研究中心成立于2003年，隶属学校，但并非保密单位。[296]在任何一个地方，安全专家和保安做的都是性质完全不同的两类工作。所以，关于斯诺登的工作性质，立刻就引起了更多的猜测。

最简单而直观的推测是，他利用自己的计算机操作天赋实现了华丽转身，从蓝领变成白领。但也有人推测，把斯诺登称为“保安”就像把“007系列”中的詹姆斯·邦德叫作“保镖”一样，那只是一种“掩盖”，斯诺登并没有什么华丽转身，他在这里只有一个身份，那就是计算机和网络安全专家，他自始至终只做了一件事情：找出这家单位的计算机系统存在的安全漏洞，避免它遭到黑客袭击。[297]

更有人搬出《马里兰州信息公开法》，要求马里兰大学提供斯诺登在这家研究中心的具体工作情况，包括“前保安”斯诺登与学校管理方的

所有电子邮件通信内容，斯诺登的岗位、任职时长、工资、上级管理者，等等。学校方面很客气地回答说，他被大学聘用的时间很短，留下的文件非常有限，并且其中还有一些属于保密资料，不能提供，但是可以提供他的工资单。终于，学校对于斯诺登的这段经历有了一个非常明确的交代：斯诺登在研究中心的经历分为两个阶段。从2005年1月28日开始，斯诺登作为无工资雇员在这里工作。没错，工资为零。此时，距离他重新登记进入安娜兰多社区学院不过几个月的时间——看来这个学院的课程对他几乎没有什么吸引力。按照原约定，这样的无工资工作将持续到8月，但是到了2005年7月，斯诺登经过申请拿到了工资。等到11月离开的时候，他一共拿到了29330美元，另外还有7%的退休金，按年薪计，约有7万多美元。至于他在这里的工作内容，白纸黑字写得清清楚楚——“安全专家”，而且从一开始就是。他离开的原因也写得很明白——“辞职”。[298]

对于他的这段工作经历，他在2006年5月是这样回忆的，其得意之情溢于言表，难免有些吹嘘的成分：

我什么学位都没有，甚至连高中文凭都没有。

也就是说，我连一分钱的学生贷款也没有，但我的年薪有7万美元。我刚刚分别拒绝了年薪8.3万美元和18万美元的职位，因为它们和我想要争取的方向不一致。我的同事都有学士学位或者硕士学位，并且还有15年的工作经验。然而，我很抢手。

我只有22岁。[299]

语言高级研究中心实在不是一家背景简单的单位。在它自己的网站上，它是这样对外介绍的：

成立于2003年，是美国国防部的大学研究中心之一……是美国国内第一家、也是唯一一家致力于解决情报界语言问题的研究单位。[300]

学校发言人说这家研究中心并非保密单位，其实也不准确。根据可以得到的照片和资料显示，这里与大学里通常来去自由的开放设施相比，算得上是戒备森严了：高耸的栅栏围成了一个独立的院落，门口24小时有人值守。2006年，美国情报界模仿军方的做法，成立了一家与国防高新研究计划局（DARPA，简称国防高新局）类似的单位，连名字都很相像，叫情报高新研究计划局（IARPA，简称情报高新局）。在情报

高新局2009年搬进新建的办公楼之前，曾“屈就”于研究中心的办公楼里。[301]因此这家中心曾有好几年作为保密单位的历史。从目前掌握的情况来看，斯诺登在情报高新局搬进研究中心之前就离开了这里。

后来，斯诺登回忆：他到语言高级研究中心工作自有其目的。这段仅仅几个月的经历有助于他获得接触绝密信息的安全许可，而绝密安全许可又是在政府单位找到好工作的敲门砖。[276]在他眼里，能到联邦政府的单位里工作是一件很体面的事情。但是，他的学历实在不够突出，不能准确地反映出他的技术天赋和技术实力。直接拿这样的学历去找工作，多半会被拒绝。以他这样的背景，在一家保密单位里获得“积分”，进而获得绝密安全许可，然后进入政府单位，是一种绝顶聪明的办法，而且斯诺登以他后来的经历告诉人们，这是一条可行的捷径：他的成功可以复制。

前面曾经提到过，美国信息系统有三种涉密级别，秘密、机密和绝密，与之相应的是三种涉密安全许可。如果想接触特密专案信息，还需要另外申请。

据统计，2012年10月，美国政府大约雇用了500万名持有某种涉密安全许可的人员，其中大约150万人持有绝密安全许可。一个人想要获得安全许可，必须通过背景审查。他必须“完整、诚实且坦白地”填写一堆表格。表格详尽到“变态”的程度——需填写姓名、学习和工作经历等通用信息的表格多达127页，填写过去10年住处、所有亲戚姓名、海外关系等特殊信息的表格也有29页。[302]

当然，申请人填写的情况是否属实还需要由专人进行审查。如果申请的是秘密或者机密许可，审查人员要到联调局调查申请人是否有案底，还要调查他的财务信用情况。如果要申请绝密许可或者特密专案许可，审查会更加严格，必须进行“单一范围背景审查”（SSBI），约谈申请人，走访他的四个关系人，甚至要和他从前的配偶面谈等。[302]

审查人员和申请人的单独会谈要用两到三个小时，主要是根据他先前填写的那些调查表提问。斯诺登很可能就会碰到类似于“为什么没有拿到学位”、“为什么那么快就从军队退役”的问题，他可以利用这个机会解释。为了得到绝密安全许可，他很可能还经过了测谎程序。[303]

2006年年中，斯诺登通过了“严格”的背景审查，拿到了绝密安全许

可，顺利进入了中情局。后来有人质疑，他怎么可能如此顺利拿到许可。一位中情局前官员指出，就获得绝密安全许可而言，他的出身和其他背景情况无懈可击，“他实在太年轻了，历史非常清白”。[279]心情愉快的斯诺登忍不住写下了下面这段“心得体会”，时间是7月21日凌晨1点刚过。值得注意的是，斯诺登在这段文字里并没有提及“中情局”，而是提了“国务院”，估计多半是出于保密方面的考虑。

想去欧洲，你可以自己想办法。

就拿国务院来说，他们现在缺人手，但欧洲的岗位很紧俏。如果你愿意去近东那些糟糕的地方，你想进去就会容易得多。一旦你进去了，咬着牙熬过那段时间，你就可以从一堆不错的岗位上选择一个了。

或者，你去申请安全许可。等你拿到许可，再加上你掌握了信息技术，而且你还有自己的生活方式，你就可以去世界上的任何一个地方。

……如果想到国务院的信息技术部门工作，你必须要有绝密安全许可……[304]

外交“随员”

斯诺登后来对英国《卫报》的记者说，他离开了马里兰大学校园后，就进入了中情局。[293]最让他吃惊的是，他原本以为技术最先进的中情局，使用的竟然是非常过时的信息技术。[15]2007年，他了解到局里正在招募精通计算机系统的人员去海外工作后，就找到上司并得到了他的大力推荐，成功地获得了那份工作。他被派往瑞士，负责中情局在那里的计算机网络安全和外交官们的计算机安全。[276, 305]瑞士外交部提供的信息是，斯诺登从2007年3月到2009年2月在美国驻日内瓦代表团工作。[306]

斯诺登为什么能“突然”从一个与国安局有关的单位跳到中情局去，这难道不是一件非常奇怪的事情吗？有人推测，斯诺登在中情局的具体工作单位很可能是特搜部。[307]

特搜部是国安局和中情局联署办公的一个部门，也就是说，这个单位既可以说属于国安局，也可以说属于中情局。基于这种推测，不仅可以解释斯诺登从语言高级研究中心转到美国驻日内瓦代表团的可行性，而且可以解释他离开瑞士后进入国安局的另一家单位的可行性。

反过来，如果斯诺登真的只是负责计算机系统的安全专家，他最多算是随员，这也是美国国务院的官方说法。以这种身份，他不应该出现在外交官名单上，但是他出现了。比较合理的一种解释是：斯诺登在瑞士的身份特殊。如果他属于特搜部的这一推测成立，那么他的身份特殊这一点自然也就成立了。

网上有一份材料称，特搜部的总部大楼位于马里兰州的贝尔茨维尔，紧挨着国务院的外交通信处大楼。在通往特搜处总部的路口有一个标识牌，上面写着“CSSG”，这是它的一个用以掩人耳目的名称——“通信系统支持处”，也是它出现在当地电话黄页上的名字。[307]在国安局的一份内部文件上是这样写的：“特搜部，或称通信系统支持处（在不涉及国安局、中情局或者情报任务时）……”这就证明网上这份材料是基本可信的。

中情局在世界各地布设了许多秘密站点，站点之间的加密通信就由

这个外交通信处来负责。特搜部的情况与之类似，他们以使馆或代表团驻地为掩护，在美国国境外建立了许多秘密监听据点，借用国务院的安全卫星信道，完成这些海外据点的通信任务。其中有一个据点就设在美国常驻日内瓦代表团大楼里，这正是斯诺登名义上的那个工作单位。[307]

关于他在特搜部工作的最重要的佐证之一还是斯诺登自己给出的。他后来对记者说：他在瑞士的工作单位是中情局的“全球通信部门”[15]——这和特搜部的掩护名称“通信系统支持处”高度契合。

说起特搜部，故事可不少。20世纪50年代，中央情报总监艾伦·杜勒斯（Allen Dulles）担心新成立的国安局成为中情局的竞争对手，便在中情局内部建立了一个迷你国安局，叫作D部门。他们甚至把国安局的元老之一、密码专家弗兰克·洛利特（Frank Rowlett）都挖了过来。不过，D部门的发展并不顺利。法律上的不允许，再加上来自联调局方面的打压，使得他们在美国国内根本无法行动，也几乎无事可做，根本达不到杜勒斯总监的预期。与此同时，他们的英国同行、军情五局的D部门在英国国内做得风生水起。几年后，洛利特又回到了国安局。[114, 308]关于洛利特，这里多说几句。他是国安局里的另一位传奇人物，早年担任过破解日军密码小组的组长，还是“二战”期间最厉害的密码机“SIGABA”的主要发明人。因为他的突出贡献，1966年，他从林登·约翰逊（Lyndon Johnson）总统手里拿到了美国情报界的最高奖项——国家安全勋章。1999年，国安局决定以他的名字命名“信息系统安全组织”总部大楼，这个组织的主要任务是研制密码。这也是国安局里第二座以个人名字命名的办公大楼，第一座是以前常务副局长路易斯·托德拉的名字命名的超级计算机大楼。[309]

洛利特走后，摆在D部门面前的出路只剩下放弃竞争、与国安局合作这一条了。他们选择了面对现实。于是，在很长一段时间里，D部门的主要任务是帮助国安局窃取对手的密码资料。1978年，这个部门变成了中情局与国安局联合下属的一个单位，也就是特搜部。中情局的情报工作能力与国安局的科技能力在这里合为一体、相得益彰。也正因为是两家联合，特搜部的领导基本上是由中情局和国安局的人轮流坐庄，国安局常务副局长布莱克就曾经当过特搜部的部长。[114]

为了完成任务，特搜部需要软硬兼施。“软”的一手靠的是可以解决掉对手的某些人，让他们把窃听器安装在计算机的键盘上，或者网络的

某个薄弱环节上，这样，国安局就可以在对手的加密软件发挥作用之前截获信息。“硬”的一手则是派人神不知鬼不觉地潜入对手所设的关键场所，把窃听器安装进去，或者直接撬开保险柜，见到什么拿什么，这种活动又叫作“黑袋”行动。[310]估计是因为溜门撬锁的人总需要带上几样工具，为了避人耳目，这些工具又总是装在黑色的口袋里，所以此类行动才有了这样的“雅号”。

窃听器、接收器以及天线等监听设备需要被做成日用品的样子，以便偷偷带到目的国。比如说，抛物天线可以伪装成一把雨伞，接收器可以伪装成一台简单的收音机或手提计算机。特搜部的工作人员总是使用隐蔽身份，带着这些“日用品”进入其他国家，然后把经过伪装的设备安装到能够进行远程控制的偏僻地点，有时候是树上，有时候是阁楼里。这些监听设备截获的信号被传输到卫星上，再由卫星传回国安局。有时，实在没有其他办法了，特搜部的工作人员甚至需要爬到电线杆上安装窃听器。[115]

特搜部做过很多“碟中谍”风格的事情。比如，给在苏联驻美大使馆窗台上栖息的鸽子身上捆绑窃听器。在美国本土以外，这个单位重要的窃听活动往往就在大使馆的某些房间里进行。[115, 311]由于这样一种工作性质，美国政府从未公开承认这个单位的存在。[312]在这个单位工作的人不隐瞒其真实身份的确不行。

关于斯诺登在瑞士的工作单位，还有一些间接的证据。在外人面前，斯诺登没有点破他在特搜部工作，但他的确谈过自己的工作情况。他的一个朋友回忆说，斯诺登说他自己负责美国大使馆的信息技术保障，需要在欧洲各地到处跑，确保美国在这些地方的大使馆通信畅通。他还为这些大使馆使用的安全平台做一些工作。[313]这说明斯诺登不仅承担美国驻日内瓦代表团的信息保障工作，还承担着这个代表团与其他美国大使馆之间的通信保障这样的技术工作。从上面描述的特搜部的工作内容来看，这更接近他们的技术人员通常扮演的角色。

斯诺登后来公布了一张幻灯片，标题是“将要部署到80个特搜部站点的vPCS”。这个“vPCS”很可能是某种安全平台。从这张幻灯片中还可以看出，特搜部在欧洲有20个左右的站点。这也印证了斯诺登所说的并非虚言：他的这份工作的确需要他跑来跑去。

总而言之，几乎可以确定，他在瑞士的工作单位就属于特搜部。当

然，这个推测是否准确，还有待将来真相大白的那一天。

在日内瓦期间，斯诺登见证了这样一件事情：中情局打算招募当地的一个银行家，于是找机会故意把他灌醉，然后让他自己开车回家。等到这个银行家因为醉酒驾车被抓，再去把他“捞”出来，最后终于达到目的，把银行家招募入局。对中情局来说，这家银行的秘密从此便不再是秘密。[293]关于这个故事的结局，还有另一个版本：银行家拒绝合作，中情局恼羞成怒，于是把他的生活彻底毁掉。[276]无论是哪种结局，在斯诺登眼里，这都是一件为人所不齿甚至可以说非常丑恶的事情。

他的身边有很多特工，强烈反对美国的中东政策和这场伊拉克战争。再加上他负责计算机和网络运维工作，这使他第一次接触到如此之多的有关这场战争的真实信息，其中很多都跟他原来看到、听到的那一套“主旋律”的东西格格不入、背道而驰。[15]年轻的斯诺登幻想破灭是迟早的事情。对此，他后来是这样说的：

我开始认识到，我的政府，在这个世界上真正所做的事情，和他们告诉我的，完全不一样。反过来，有了这样一种认识，你就会开始重新考虑你看待事情的方法，更多地怀疑这些事情。[276]

“盟友未必是朋友”

2013年10月，《明镜》周刊刊登了一条爆炸性新闻：德国总理安格拉·默克尔（Angela Merkel）被美国监听超过10年，监听据点设在美国驻德大使馆，负责监听的就是特搜部。作为监听据点，这个大使馆的确非常理想：它地处德国的政治中心地带，距离德国议会大厦只有几步之遥，抬头就能看见勃兰登堡门。[314]

让美国大使馆建在这样一个位置，可以看出德国人是发自内心地信任美国人——他们真把美国人当作了自己的朋友。就在5年前，大使馆落成，美国人举办了规模盛大的超级派对，各方的贵宾来了4500多人，老布什前来剪彩，默克尔也亲自到场助兴，还发表了热情洋溢的讲话。[314]默克尔原本对奥巴马的印象也不错，2011年她还得到过由他颁发的总统自由勋章。[315]过去的这一切显得如此温馨和谐，但到了秘密揭穿的这一刻，却显得如此滑稽可笑。德国安全部门对此毫无察觉、毫不设防，因为他们认为朋友之间不需要如此紧张、如此保持警觉。

因为害怕误会美国人，《明镜》周刊专门请来了英国的调查记者邓肯·坎贝尔（Duncan Campbell），他在揭秘圈里可是个名人。坎贝尔很快发现，美国大使馆屋顶上的阁楼有个像窗户似的凹口，没有安装玻璃，而是罩了一层特殊材料。他说，特搜部的侦听设备就安装在这层薄膜之下。《明镜》周刊还是不踏实，又把班福德请来，他的看法和坎贝尔一样：“国安局的侦听设备就藏在下面，他们在更大的系统上也使用过这种防护材料。”[314]

紧接着，美国人监听默克尔的“铁证”被公布了出来。这是一张发黄的纸片，一眼看上去像是从某个数据库中输出的一条记录，可以一行一行，也就是一个字段一个字段地解读。在“筛选值”那一行，被涂黑的那一块就是默克尔被监听的那个手机号码。经德方确认，总理主要用这个号码联系她的私人朋友。美国人很严谨，他们怕出错，便在默克尔的名字前面特意标注了“德国总理”这几个字。

在这张纸片上，在“提出监听需求的单位”（Ropi）一栏填的是“S2C32”，这是国安局内部的部门代号，“S2”代表信号分局分析产品

部（也有一说是采购评估部[314]），“C32”指欧洲产品线。也就是说，对默克尔进行监听的命令来自国安局的欧洲产品线，这个部门属于信号分局的分析产品部。

“国家信号情报需求清单”（NSRL），即美国人设定的监视目标清单，这一栏填的是“2002-388”，可以推测是指“2002年第388号”。也就是说，对默克尔的监听开始于2002年。那一年，伊拉克正处于日益迫近的战争边缘，德国对此事的态度不同于美国，这让美国人颇为不快。就在那一年，德国国内进行议会选举，默克尔向总理宝座发起了冲击，不过没有成功。

接下来的“状态”（Status）一栏里是字母“A”，代表“激活”（active）。也就是说，在这条记录输出的时候，对默克尔总理的监视还在进行之中。据《明镜》周刊称，这条记录输出的时间大约就在2013年6月奥巴马访问柏林的几周之前。[314]

最后一栏是对默克尔实施监听的单位“重要目标办公室”（Topi），后面填的是“F666E”，“F6”指的就是特搜部。

对默克尔来说，她的手机不仅仅是手机，还是她指挥政党、领导政府、行使权力的工具。她也非常依赖这种通信工具，是出了名的“短信控”。据说，她可以一边说话，一边给屋里的其他人发短信。[316]德国政府甚至还讨论过，是否应该把她的短信看作一种政府行为，进行存档。默克尔则经常半开玩笑半当真地说，她的手机正在被人监视。她当时头脑里想到的多半不是美国人，因为他们是德国人的朋友。[314]

得知自己从10多年前就开始被监听，默克尔肯定感觉像被人从背后捅了一刀。极为恼怒的她马上拨通了奥巴马的电话，厉声质问他这是怎么一回事。奥巴马赶紧解释，他对此一无所知，而且保证，现在没有、将来也不会监听默克尔。据调查，对于默克尔的这次行动，62%的德国人表示支持，但也有25%的德国人认为他们的总理还是太过温和了。[314]

德国人当然不傻。此时此刻，要让他们相信奥巴马不知道此事非常困难，更何况有人向他们知会说，奥巴马早在2010年就知道国安局监听默克尔这回事了。当时是亚历山大局长做的汇报，但总统并没有下令停止行动，局长得到的命令是：继续行动。[317]据说，奥巴马对默克尔

并不信任，他曾经要求国安局准备一份详尽的默克尔档案，把她的所有情况都调查清楚。[318]默克尔看到这些报道的时候，多半会联想到另一件事：在奥巴马下达这些命令一年之后，他居然给她颁发了一枚总统自由勋章，这是一种什么心态呢？同时获勋的还有美国前总统老布什和“股神”沃伦·巴菲特（Warren Buffett），这又是一种多么奇怪的组合呢？

当然，国安局对于这些报道是完全不会承认的。[319]但国安局前局长海顿在接受《明镜》周刊采访时说了下面这样一段话，听上去更加实事求是：

我们的政府已经明确表态，总统不知道。我也只能说，如果总统说他不知道，他就是不知道。但是白宫不可能不知道，国家安全委员会不可能不知道。当然，这不是总统一个人的决定。[320]

怒气未消的默克尔总理在欧盟峰会上恨恨地甩出一句话：“朋友之间搞监听，没人这么干过。”[314]话音未落，角落里就传来一个幽幽的声音——“盟友未必是朋友”。说这话的人叫斯图尔特·贝克尔（Stewart Baker），曾在麦康奈尔担任国安局局长期间担任局里的法务长，后来成为国土安全部第一任负责政策的助理部长。[321， 322]他非常直白地道出了默克尔总理以及她的前任格哈德·施罗德（Gerhard Schröder）成为美国人监视对象的根本原因：

我们通常视作朋友的那些国家，某些时候的所作所为其实非常蓄意地伤害了美国和美国的利益。10年前，美国要去和伊拉克打仗，法国和德国就不是我们的盟友，甚至连中立都算不上。他们积极地和俄罗斯与中国走到一起，阻挠美国的军事行动。他们将来还会不会违背美国的意愿行事呢？

奥巴马和他的政府是这个世界上几乎所有国家的情报目标，其中就包括叫得最凶的那些国家……这就是生活，这就是国际政治。德国总理默克尔对此非常熟悉。

美国如果停止搜集情报，它就会面临可怕的突袭，所以它的情报搜集不会停歇。[321]

就连班福德都说，美国政府对德国“感兴趣”可以理解，既因为德国的政治和经济影响力，也因为当年的“9·11”事件就是在德国汉堡附近的

哈尔堡酝酿而成的。[323]

到这个时候，德国人其实不应该再期盼奥巴马会出来说点儿什么、做点儿什么了。果然，美国总统对此“不置一词，周日还去参观了一家教堂，打了四个小时的高尔夫球”[322]。

贝克尔的那句“盟友未必是朋友”虽然是往德国人的伤口上撒了把盐，但也真的成了点醒德国人的“警世通言”。总而言之，在这样的事实教育下，从幻想中清醒过来的绝不仅是涉世未深的斯诺登，还有广大德国人。有理由相信，从此以后，美德关系将进入一个更现实、更理性的新阶段。

德国ARD电视台的记者发现，就在默克尔和奥巴马通话后的第二天，美国大使馆阁楼上那块“窗户”发射的红外信号大幅减少，说明隐藏在里面的监听设备从那时起很可能停止了运作。[324]看来，默克尔的那通电话还是起了一点儿作用。

特搜部的这些监听活动有个代号——“特等舱”。他们在全球建立了80个据点，其中欧洲有19个，日内瓦、布拉格、马德里、巴黎各有一个，德国被特别关照，在柏林和法兰克福分别设置了一个，并且配备了最先进的设备。比如，他们使用了一种天线系统，代号“爱因斯坦”，而与之配套的一种控制装置，代号“响板”。[325]

回忆起在瑞士的那段日子，斯诺登说：

我对我的政府如何使用权力，以及这个政府在世界的影响等方面原本抱有幻想，但我在日内瓦看到了很多事情，我的幻想破灭了。我意识到自己是作恶多于行善的某种东西的一部分。[293]

在日内瓦期间，他脑子里第一次萌发了要揭秘的念头。这可是一个大得吓人的决定。一番犹豫之后，他决定再等等，因为他不希望他的揭秘伤害到某个具体的人，而中情局的黑幕绝大多数都会涉及个人。2008年奥巴马当选新一任美国总统。在就职典礼上，他宣誓说，要改变那些借“反恐战争”正名的权力滥用现状。斯诺登希望这位新总统能够说到做到，进行真正的改革、带来真正的改变，这样那些秘密就不需要去揭开了。[276, 293]当然，斯诺登说的这些也可能不全是实话。他当时对共和党候选人约翰·麦凯恩（John McCain）印象颇深，对奥巴马并没有特别的好感。

尽管斯诺登心情如此，却也没有影响他技术水平的发挥和提升。他在简历里提到，自己这段时间一再被派去执行临时任务[326]，其中就包括在2008年北约峰会期间，他被点名派到罗马尼亚为总统服务[276]。看上去他在中情局还有升职的可能，但这种可能性不久就破灭了，正应了一句古话“祸从口出”。年轻气盛的斯诺登和某个高管意见不一，发生了口角。他可能并没有太在意这次“电子邮件小争吵”，以为事情就此过去了。几个月后，斯诺登偶然发现了局里的人力资源软件有一个漏洞，在自己的团队和直接上司的支持下，他试着修补漏洞。没想到曾经与他有过口角的那位高管却因为这点儿小事借题发挥、上纲上线，不客气地在斯诺登的个人档案上写了一个“恶评”，理由是：疑似未经授权，接触涉密文件。斯诺登第一次感受到：想在体制内解决问题，除了结果不会太妙，还很可能给个人惹上麻烦。[327]等到斯诺登事件发生，面对媒体质询，中情局终于发声，首次承认斯诺登曾经为自己工作，但对于他的这次“恶评”经历全盘否认。[328]

这件事情改变了斯诺登，原先那个温和的斯诺登变成了另外一个人。2009年1月，《纽约时报》上刊登了一篇报道，披露了以色列进攻伊朗的秘密计划，斯诺登看了以后义愤填膺：

“《纽约时报》太过分！他们是想挑起战争吗？”

“他们把秘密都捅出来了。”

“是哪儿来的匿名家伙告诉他们这些事情的？这些浑蛋就该被惩处。”[305]

也许这才是他的心声，也许不是。谁知道呢？

由于那个“恶评”，斯诺登必须面对没完没了的调查，除非他离开中情局。心灰意冷的斯诺登决意离开日内瓦。瑞士带给了斯诺登富足的物质生活，政府分给他住的公寓有四个房间，就在日内瓦湖边。他还为自己购置了一辆崭新的宝马车，为了畅快飙车，他甚至拆掉了车上的电子限速器。[279]对年轻的斯诺登而言，这并不仅仅是一段如诗如画、风光无限的异国之旅，更是一段充满矛盾、充满拷问的良心之旅。[329]这个年轻人显然还没有做好准备：尽管他的内心受到了冲击，在认识上开始出现怀疑，但还没有彻底到价值观崩溃的地步。事后来看，他在这段时间其实还未开始搜集和积累资料，这些准备工作要等到接下来的几

年时间去做了。

心“移”之地

2009年，斯诺登离开瑞士回到了美国，情绪仍然不能平复。现实生活中的他只能有所收敛，网络世界中的他则更为本真。这段时间，论坛上如果有人胆敢挑战他的看法，他马上以“弱智、浑蛋”回敬。[279]好在很快他就在戴尔公司找到了一份新工作，地点是美军驻日基地里的一家国安局单位。看上去中情局的那个“恶评”并没有影响他找到这份新的工作。他在戴尔公司一干就是三年多。经过这次工作单位的变迁，斯诺登本人也完整地经历了一次“旋转门”的过程。

到日本工作的确能使斯诺登换换心情，因为这里是他很喜欢的一个地方。十几岁的时候他甚至学了一年半的日语，这对于一个讨厌学校教育的少年而言实属不易。他的朋友仍然记得，他会时不时把自己称作“Edowado”——这是日语版“爱德华”的读音。[287]按时下流行的说法，可以把他算作“哈日”一族。对于自己的未来，他18岁时，曾经做过这样的展望：

我一直梦想着能够在日本“取得成功”。我非常希望能够在那儿找到一份轻松的在政府部门的工作。[305]

有材料说，日本一段是斯诺登人生的转折点。[330]在这里究竟发生了什么？他在这里又做了什么呢？

斯诺登在这里开始了一段真正意义上的恋爱——他的女友米尔斯搬来和他住到了一起。[331]据他们的朋友说，他们俩是在2005年前后在马里兰州认识的，米尔斯那时在一家女子健身中心里做钢管舞教练。[280]两个人都疯狂迷恋日本的街头表演艺术[306]，当然还有卡拉OK和日本美食。后来，到了夏威夷，俩人还经常跑出去K歌、享用寿司和天妇罗。[332]

斯诺登对于自己的工作内容，从来都守口如瓶，对于在日本的工作情况也不例外。无论他面对的是记者，还是女友，都是如此。虽然已同居多年，但在米尔斯面前，他仍然是一个不折不扣的神秘人。在自己的微博上，她把斯诺登叫作“E”、“我的神秘男人”。在一个帖子中，她说自己很高兴，终于把斯诺登本人带到了她的朋友面前，她的这些朋友对于

这个“E”是否真的存在一直将信将疑。[333]

要理解斯诺登的心路历程，很重要的一件事情就是把他工作过的这家美军驻日基地的状况弄清楚。根据公开资料，国安局在日本只有一家信号情报站，就设在三泽美国空军基地里，所以把这里当作斯诺登在日本工作的地点，完全符合媒体上宣称的“他在美军驻日基地为国安局工作”这样一个别别扭扭又神神秘秘的说法。[293]

三泽基地位于日本本州岛北端的青森县三泽市（日语写作“三沢”），是美国空军35飞行联队的大本营。除了这个飞行联队，还有一个叫作“三泽安全行动中心”（MSOC）的神秘单位在这里驻扎。这个安全行动中心的成员来自美军的多个军种和兵种。行动中心下辖空军373情报监视侦察大队和301情报中队、海军三泽信息行动指挥部、陆军708军事情报分队。[334]2009年前后，属于这个中心的还有海军陆战队支援营的一个排。[335]

2014年2月，美国国防部宣布进一步压缩预算，陆军受到的冲击最大，52万人最终将被压缩到44万～45万，这将是美军自1940年以来规模最小的一支陆军。[336]仅仅几天之后，三泽基地的官网上就登出一条消息：计划到2015财年年底减员500人，届时，基地的军人总数将减至3100人。这次缩编对安全行动中心也有直接的影响。[334]

首先被裁减的是陆军708分队。按计划，这支有着50年历史的分队将于2014年10月解散。它的命运是近几十年美国陆军历史的一个缩影。1964年陆军安全局403特种行动分队成立，这就是708分队的前身。这个分队的部分人员后来辗转到了三泽情报分队，1982年扩编成750军事情报营。在这支陆军部队里，信号收集与鉴别分析人员的代号为“98K”，他们把数字信号破译成可辨识的信号，接下来的情报开发任务就要由信号情报分析人员（代号“98C”）、语音情报监听人员（代号“98G”）、通信信息定位和监听人员（代号“98H”）以及电子情报监听和分析人员（代号“98I”）来完成了。随着冷战结束，情报营很快就被压缩为连，再被压缩为分队，然后又被改为403分队、708分队，最终它们在这次裁军中被解散。[114, 337]

算起来，这家神秘的安全行动中心已经成立60多年，2003年之前它的番号是“三泽密码行动中心”（MCOC）。早些年，中心里来自美军各军种的军人曾经达到1800人，这还不算在这里工作的各类地方人员。到

2003年，军队和地方两类人员的总数减少到900人，其中大约一半是25岁以下的年轻人，其中也包括像斯诺登这样的为国安局工作的公司雇员。[114, 338]

行动中心的驻地叫作安全山，山坡上散布着十几架巨大的球状天线，但真正的地标性建筑是AN/FLR-9天线阵，这个围成三圈的庞然大物高137英尺（近42米）、占地39英亩（大约15万平方米），被形象地称为“象笼”。天线阵于1963年动工，两年后完工，当时的主要任务是监听苏联和中国的无线电通信。[339]从技术上讲，AN/FLR-9又被称为环形配置天线阵（CDAA），从30千赫兹的极低频（VLF）信号到30兆赫兹的极高频（VHF）信号都是它的监听对象，监听距离为150~5000千米，围成三圈的天线分别用于接收三个频段的信号。这些信号主要由对方空军使用，因而侦听这些信号顺理成章地成为美国空军信号情报部队的任务，天线阵也就主要由他们使用。除了三泽，美国人在其英国、泰国、菲律宾、意大利和土耳其等地的空军基地都建起了这样的天线阵，所有这些AN/FLR-9天线阵合起来被称作“火车头”计划。但是，除此之外，安全行动中心还另有一项更为重要的任务。

这项任务要靠山坡上那些球状天线来完成。其实，说它们是“球状天线”并不准确，那些像高尔夫球一样的东西只是天线罩，在它们的内部有一个碟状天线，它们的侦听对象是太空中的卫星。和“象笼”天线阵类似，这样的球状天线阵也不止架设在三泽这一处。不同的是，这些天线阵并不总是由美国人来操作。美国人找到了四个铁杆盟友，他们合起来被叫作“五只眼”。所有这些天线阵合在一起也有一个名字，叫作“梯队”计划。[340]有关这个计划的内容，后面将会详细介绍。在这个计划里，三泽安全行动中心的代号是“情人”。

三泽基地是美国国安局在海外布下的一颗重要棋子，参与了国安局的诸多情报搜集行动，非常像斯诺登的工作地点。可是，据斯诺登自己说，他在日本的工作地点并非三泽基地，而是横田空军基地。如此看来，国安局在横田基地里也安插了一个情报单位，不过这个单位更为神秘，到目前为止，有关其参与的情报行动没有任何材料被公开，只能等以后再来揭秘了。

平心而论，斯诺登在基地的工作还是尽心尽力的。他甚至开发出了一个极其复杂的容灾备份系统“EPICSHELTER”。有了它，即使国安局的某个站点遇到某种意外灾难，国安局也可以从其他站点找回原始数据。

[279]2010年9月，斯诺登飞到印度，在Koenig培训班上学习了6天的黑客技术，例如怎样入侵计算机系统、怎样抹去入侵痕迹，他最终获得了国际电子商务咨询公司（EC-Council）授予的“道德黑客”认证。[341]这种认证要求黑客对他们检查系统漏洞时发现的机密信息进行保密。斯诺登的工作职责也从仅负责计算机系统升级，扩展到担任“赛博战略家”和“赛博反情报专家”。[326]但随着他了解到的情况越来越多，他内心失望、不安和不满的情绪也在滋生和膨胀：

我看到，奥巴马推进的每项政策恰恰是我认为应该有所收敛的。[305]

斯诺登在这里看到，国安局的监视活动无所不用其极，而对这些活动进行约束的机制全都在空转，这些都与他曾经接受的思想教育、树立的理想信念背道而驰。终于，他下定决心要做点儿事情。几年以后，面对记者，他是这样回忆的：

国安局建立起来的基础设施足以支持它侦听所有事情。他们的能力允许他们把全人类的通信记录自动地摄录下来，根本不需要事先确定某个目标。如果我想查看你的电子邮件，或者看你妻子的手机，我需要做的就是侦听。我可以得到你的电子邮件、密码、电话记录和信用卡记录。

面对国会提出的“美国本土的侦听范围到底有多大”这样一个问题，国安局习惯性地撒谎。我相信参议员罗纳德·怀登（Ronald Wyden）和马克·尤德尔（Mark Udall）肯定提出过这样的问题。国安局的回答是，由于没有工具，无法给出问题的答案。但我们真的有这样的工具，我有一份地图，它能显示出什么地方的人被审查得最厉害——我们搜集美国人的数字通信信息比我们搜集俄国人的还要多。

我们可以在机器里植入窃听装置。一旦你上网，我就可以发现你的机器。不管你采用什么样的防护手段，都再无安全可言。

2008年，许多人都投奥巴马的票。我没有。我投给了第三党，但是我相信了他的承诺。事实上，他却继承了他前任的政策，所以我决定揭露这些秘密。[342]

2012年3月，斯诺登离开日本。几个月后，三泽基地对外宣布，将在2013年拆除陈旧的地标性建筑“象笼”。安装在冲绳读谷村的另外一

个“象笼”则早在2007年就拆除了。三泽的“象笼”被拆掉后，全世界就只剩下最后一个“象笼”还在运作——它孤独地耸立在天寒地冻的阿拉斯加。[339]

“库尼亚坑道”

斯诺登回到了美国，并非离职，只是工作调动——他依然是戴尔公司的雇员。具体工作地点不得而知，只知道是国安局在马里兰州的一家机构，他的主要工作是跟微软和其他公司的员工一起，为情报部门打造安全的计算机文件和数据存储系统。在这里，他亲眼看到国安局和私营企业联手获取普通民众的通信记录。[276]

斯诺登这次在马里兰的工作时间并不长。不久，他的工作再次变动。这一回，他作为系统管理员，前往夏威夷，工作单位换成了中安局（CSS，中央安全局）下面的夏威夷“区域安全行动中心”（RSOC）。这个单位有好几个名字，“区域信号情报行动中心”、“区域密码中心”等。官方事后调查发现，斯诺登大约从2012年4月开始下载国安局敏感文件，[330]大概就是他进入这家单位工作前后。据亚历山大局长介绍，在斯诺登进入博艾汉公司前，曾在国安局的某个岗位上工作了一年，其间得到过特密专案许可。他提到的这个岗位，应该就属于这家单位。

国安局和中安局名称里都有的“安全”一词，大抵就是“信号情报”的意思，用“安全”取代“情报”两个字，可以减轻其对人们神经的刺激和冲击。“国安局”就是美国的国家信号情报局，而“中安局”就是美军的信号情报局。在美国，“国家”层面的信号情报工作几乎完全依靠“军队”层面的人员和设备来完成，所以国安局和中安局这两家单位是两个牌子、一套班子，国安局局长兼任中安局局长。从任务上看，中安局主要完成军队特有的信号情报任务，比如针对外方军队信号情报的侦听、干扰和对抗。借助于他们的徽章可以更直观地说明这些事情。中安局的徽章分为6个部分，处于中心位置的是国安局和中安局机关，用的就是国安局徽章图案。从五角星的1点钟位置开始，顺时针一路看下去，分别是空军情报监视侦察局、海军舰队赛博司令部、海军陆战队情报主任、海岸警卫队情报助理指挥长和陆军情报与安全司令部五个单位的徽章图案。[343]按照班福德的说法，中安局就是国安局自己的海陆空三军。[137]作为国安局局长，亚历山大的权力还不仅于此：他同时兼任美军赛博司令部的司令，手下管理着三支部队——海军第10舰队、空军第24航空队和陆军第2军[344]，这三支部队又分别被称为各自军种的赛博司令部。他位高权重，同僚们难免有些羡慕和嫉妒。中情局的一位前高级官员就

说，大家私下里半开玩笑地把局长叫作“亚历山大大帝”，因为无论他想要什么，他总能得到。[344]

夏威夷“区域安全行动中心”的历史可以追溯到“二战”。“珍珠港事件”之后，在檀香山以西的一片开阔土地上，美军建起了一座隐蔽性很好的坚固工事，当地人把它称作“地洞”，美军自己把它称为“库尼亚坑道”，其实这些名称都不太准确，它实际上是一座25万平方英尺（大约2.3万平方米）的三层楼，建好之后用土掩埋，只留下一个出口。它最早被用作飞机组装机库，几经加固、转换交接，最终成为侦听中国和朝鲜信号情报的前哨阵地。[345]就在斯诺登到这里工作之前的几个月，2012年1月，行动中心正式启用了新的办公大楼，大楼被命名为“罗什福尔”，纪念曾经在这里工作过的约瑟夫·罗什福尔（Joseph Rochefort）上校，他所带领的密码团队为取得中途岛海战的胜利立下汗马功劳。[346]新楼占地70英亩（大约28.3万平方米），建筑面积和“坑道”差不多，内设指挥中心、行动汇报中心、数据分析区，以及多个任务计划区和电视电话会议区。[347]

尽管新大楼已经启用，但不知道为什么斯诺登仍在阴冷的“库尼亚坑道”里工作。[279]表面上看，斯诺登跟其他在这里工作的人员一样，按时上下班、沉默寡言，甚至没有人注意到他经常穿着一件黑色的外套，外套上有一个醒目的经过篡改的国安局徽章。正版国安局徽章上的老鹰雄赳赳地抓着一把钥匙，寓意是掌握密钥，密钥是信号情报工作取得成功的主要途径，因此几乎所有信号情报单位的图标上都会出现一把钥匙。而在修改版的徽章上，老鹰两眼通红、头戴耳机，抓着的是美国电话电报公司的电缆，显得滑稽、笨拙，讽刺国安局的意味十足。[278]这个徽章以及外套的设计者是著名的“电子前沿基金会”，他们的口号是“保护你在数字世界的权利”。斯诺登选中这样一件外套，显然是想表达一些东西，但他身边的同事以及上司都没有太在意。他后来说过这样一段话，可以看作他的心声：

丘奇曾把（情报部门滥用权力）这种情形比作身处深渊的边缘，他非常担心，一旦我们跌入这个深渊就再也出不来了。我们现在的担心是，我们再次处在深渊的边缘。[15]

斯诺登知道，要解决政府部门滥用权力的问题，唯一的办法是向世人曝光这些丑恶行径，丘奇当年就是这样做的。不过，他不能像丘奇那样大张旗鼓地行事，他只能悄悄行动。[15]

事后调查发现，斯诺登交给媒体的文件绝大多数不是手动下载的，而是借用了一种称作“网络爬虫”或者叫“网络蜘蛛”的计算机软件。[348]这种软件的技术原理和搜索引擎类似：它能自动分析出网页上包含的链接信息，并且顺着这些链接信息“爬”过去，把更多的网页或者文件抓取下来，最终可以把整个网上的信息都抓下来——只要有足够大的存储空间。他抓取文件的源头，是国安局内部非常重要的一个站点，叫作“维基”（wiki）。

受“维基百科”的启发，美国情报界在2005年正式建立了自己的维基“情报百科”（Intellipedia），使用了与“维基百科”相同的软件。根据涉密程度，分为三个不同板块。[349]到2014年1月底，绝密级板块拥有注册用户25.5万、网页11.3万、被阅读次数超过2.9亿，秘密级板块有注册用户21.4万、网页10.7万、被阅读次数超过2.4亿，而非密级板块有注册用户12.7万、网页4.8万、被阅读次数超过949万。[350]

斯诺登到底复制拿走了多少涉密文件，亚历山大局长的估计是5万～20万份，[351]国安局“斯诺登事件”调查小组组长理查德·莱杰特（Richard Ledgett）的估计则是170万份。[352]后来，班福德在采访斯诺登时，也提起了这个问题。斯诺登说，他在复制文件的时候，试图留下数字“面包屑”，以便国安局的调查人员日后能循着这些“面包屑”去了解他带走了哪些文件、哪些文件他只是“碰过”但并没有带走。但国安局并没有发现他留下的这些记号，莱杰特所说的“170万”是他“碰过”的文件数量，实际上他带走的远远小于这个数字。[15]

调查显示，斯诺登披露的文件主要来源于国安局内部的维基。[348]关于这个内部维基的用户数和网页数等信息，现在还不得而知。但是，根据上面提到的情报界维基的数量规模，以及斯诺登对班福德说的这段话，可以认为亚历山大局长的判断更准确一些。

有人说，像斯诺登这样大量地抓取文件，如果是在国安局总部，几乎不可能实现。因为总部安装了先进的监控系统，遇到这样的情况就会自动报警。斯诺登是在山高皇帝远的夏威夷，那里还没有安装监控系统，所以他才能得手。即便如此，斯诺登还是遇到过麻烦，毕竟这样大规模地下载，系统总会显示出某些异常。面对官员的质询，他的回答从容镇静、滴水不漏：因为他当时的身份是系统管理员，需要进行例行的系统维护和数据备份工作。[348]

除了直接“抓取”国安局维基上的文件，斯诺登还借助一种叫作“脏词搜索”的办法来获取更多的文件。所谓“脏词”，就是官方认为不应该在计算机系统中存在的敏感词。如果发现了包含这些词汇的文件，系统管理员就有责任把它们清理掉，以保持系统的“清洁”。和系统维护、数据备份一样，脏词搜索也是系统管理员的一项例行工作。[327]

斯诺登知道，掌握了这么多文件，把它们胡乱堆在一起可不行。他快速地阅读了这些材料，仔细地分类，把这些文件放在不同的文件夹里，文件夹里再嵌套子文件夹。[353]为了整理这些文件，他一定花费了很多时间。

一次，斯诺登在搜索结果中发现了一份国安局总监察官报告，“这份报告的密级超出了系统允许的最高涉密等级”，好奇心驱使他打开文件浏览。尽管还不是终稿，这份文件却已把“星风”行动的来龙去脉写得清清楚楚。读完之后，斯诺登坚信，这个高度机密的行动是非法的。他在后来接受《纽约时报》记者专访时说：

如果政府的最高官员都在破坏法律，毫不担心会因此受到惩罚，也毫不顾忌可能产生的反响，那秘密的力量将变得极其危险。[327]

到这个时候，斯诺登仍在尝试在体制内解决问题，他先后找过十多个上级主管，向他们报告政府过度监视的问题，但没有得到任何回应。他还给上级写过很多封电子邮件，也都石沉大海。事后，国安局调查小组对此均拒不承认。[279]摆在斯诺登面前的只剩下一种选择：通过新闻媒体把这些文件公布出来。

决裂

斯诺登准备了一份媒体记者名单，排在前面的人中，有一位叫格林沃德，另一位叫劳拉·波伊特拉斯（Laura Poitras）。说到这位波伊特拉斯，她本身就是一本故事书。她出生于波士顿城外的一个富裕家庭，高中毕业后却出人意料地跑到旧金山的一家高级餐馆里当起了厨师，更出人意料地是她在那里学会了拍摄电影，后来她回到东海岸，在纽约以拍摄电影为生。[354]

波伊特拉斯拍摄过一部很有影响的纪录片，《伊拉克，我的祖国》，讲述伊拉克民众在美军占领下的生活。[279]为了拍摄这部影片，她冒险在武装冲突最为严重的逊尼派三角地待了近8个月，功夫不负有心人，影片最终获得奥斯卡金像奖和艾美奖的提名。[353, 355]接下来，她拍摄了反映关塔那摩囚犯状况的纪录片《誓言》，在圣丹斯电影节上获奖。她打算再接再厉，再拍一部，和前两部一起构成“美国新世纪”三部曲。不过，她并没有立即着手实现自己的这个想法，而是抽空拍了一部涉及国安局“星风”行动的短片——《那个计划》。谁也没想到，她拍的这些影片给自己带来了巨大的麻烦。她的机票上被悄悄打上了一个特殊的“二级安全筛查对象”（SSSS）标记，意思是说需要对她进行额外的安全检查。[354]

“9·11”事件之后，美国政府编制了两份涉及航空安全的“黑名单”。一份叫“禁飞名单”，被列在上面的人不允许乘坐飞机进出美国。名单上面原本有一万多人，2012年突然增加到两万多人，其中大约只有500人是美国人。[356]第二份黑名单就是“二级安全筛查对象”，2009年这份名单上有1.4万人。[357]于是乎，波伊特拉斯进出美国时屡屡受到特殊对待，先后在机场被扣留过近40次。[353]不仅在美国如此，有一次她从波斯尼亚飞往奥地利，在维也纳机场被单独扣下来接受检查，工作人员告诉她，是美国政府提出来要求他们这么做的。她开始给国会议员写信反映情况，但问题一点儿都没有解决。[354]

波伊特拉斯的遭遇惹恼了另外一位记者，他就是格林沃德。“路见不平一声吼”，格林沃德很快就写好了一篇文章，发表在《沙龙》杂志上，把女记者受到的不公正待遇公之于众。格林沃德文笔犀利，文章的反响

强烈。说来也奇怪，他的这篇文章发表之后，波伊特拉斯进出美国再没有碰到过麻烦。[353]对她长达6年的骚扰和监视到此才算暂时告一段落。[354]这篇文章给斯诺登留下了深刻印象，他也从此记住了这两个名字，把他们作为优先联系的对象。后来斯诺登有过这样一段回忆：

波伊特拉斯和格林沃德是这个时期屈指可数的勇敢记者，他们能够直面针对个人的苛责，毫不畏惧地报道带有争议性的话题。波伊特拉斯甚至还成为最近披露的那些计划的（监视）目标。她兼具勇气、经验和才能，这些是接受最危险任务（揭露世界上最强大的政府所干的秘密勾当）的记者必须具备的，这些使她成为（我的）当然人选。[354]

2012年感恩节前后，斯诺登的女友米尔斯回马里兰州去了，屋里终于安静了下来。斯诺登打开了自己的计算机，化名为“辛辛纳图斯”（Cincinnatus）给格林沃德发出了第一封电子邮件。这一天是12月1日。辛辛纳图斯是古罗马的一个执政官，他带领民众抵御侵略，在打败敌人后主动放弃权力，解甲归田，留下一段佳话，被誉为“公民道德典范”。斯诺登知道格林沃德没有PGP公钥，便非常诚恳地写下了第一封信，苦口婆心地劝他安装必要的PGP软件，以便给他传递一些敏感材料。信中写道：

你可能愿意从有些人那里了解情况，可是如果不能确保信息传递过程中不被监视，他们是绝对不会联系你的。[358]

可是，警惕的斯诺登并没有在信中透露任何具体线索，格林沃德一想到安装PGP软件就有点儿发怵，也就没有停下手头的工作。三天后，斯诺登来信询问。格林沃德迅速回复“准备动手落实”。斯诺登收到邮件后非常兴奋，马上发过来一份操作指南，没想到在格林沃德眼里，这份指南有如天书，他根本看不懂，此事便又被搁置。[353]

几天之后，12月11日，斯诺登主持了一个草根密码晚会，培训普通人如何利用软件对付监视。他成功邀请到了鲁娜·桑德维克（Runa Sandvik）到晚会现场给大家上了一课。她是著名的“洋葱头”（TOR）软件社区的重要成员。桑德维克讲解完如何使用“洋葱头”之后，斯诺登用三四十分钟时间介绍了“TrueCrpyt”的用法，这是一种开源软件，可以对整个硬盘或者U盘上的数据进行加密。为了组织这场晚会，斯诺登留下了自己的联系方式，就是他以“辛辛纳图斯”署名的那个邮箱（cincinnatus@lavabit.com）。[359]

这边晚会开得很热闹，那边格林沃德却是一点儿动静都没有。2013年1月底，斯诺登终于收到了他的一封邮件，信中说，他有望两三天内处理好此事。斯诺登很高兴，回信说：

这是个好消息！如果将来需要进一步帮助或者碰到任何问题，欢迎随时提出。请接受我对你支持通信私密所表达的最衷心的感谢！[358]

他还制作了一个视频短片，题为“记者使用PGP指南”，发给了格林沃德，可接下来就又没有动静了。斯诺登明白，格林沃德还是没有采取行动。两个月的时间很快就要过去，事情却一点儿进展都没有，斯诺登内心十分沮丧。[353]他事后回忆说：

我这边已经做好准备，牺牲自由，甚至搭上性命，把几千份来自美国最隐秘情报单位的绝密文件交给他——这样的爆料可能带来几十条甚至上百条的爆炸性新闻，可是他那边却不愿意费点儿劲儿安装一个加密程序。[353]

让斯诺登内心不安的还有一件事：他发现自己手中的资料无论是在数量上还是在质量上，都还不够分量，而要想得到更多资料，他需要得到更大的安全授权。斯诺登很清楚，博艾汉公司是国安局业务外包的主要承包商之一，有机会接触到更多重量级的资料，于是他决定到这家公司去试一试。[331]的确，博艾汉公司提供很多涉及国安局业务的重要工作岗位，斯诺登在这些岗位中进行了挑选。他拒绝了“特别接入行动处”（TAO，简称特接处）的工作邀请，接受了“威胁行动中心”提供的一个职位。[278]这家单位位于檀香山市的中心地段，占据金融区一栋大楼的整整一层，和他先前工作的“坑道”形成了鲜明的对比。[331]

从3月30日开始，斯诺登在国安局总部接受了为期两周的培训，4月中旬他飞回夏威夷。[279]斯诺登原本只是希望在“威胁行动中心”期间能够掌握国安局在全世界非法侵入计算机的证据[360]，结果他的收获远远超出了预期。就在他离开公司的前几天，斯诺登得到了涉及“棱镜”计划等国安局极不愿意公开的文件。

在这段时间，斯诺登联系上了波伊特拉斯。和倔头倔脑的格林沃德不同，她早就在使用PGP了。除了PGP的保护，斯诺登还指导她建立起更安全的通信环境。[354]刚开始，波伊特拉斯比斯诺登还紧张：

我（对他）说，或者你真的有这样的（敏感）信息，你正面对巨大

的危险，或者你在给我和我认识的人设套，或者你就是个疯子。[354]

不久，波伊特拉斯收到一封加密邮件，上面罗列了许多个政府正在进行的秘密监视计划，其中只有一个名字她听说过，剩下的则闻所未闻。斯诺登告诉她，他手里有每个计划的证据。看完邮件，波伊特拉斯首先做的就是切断网络、删除邮件。“他说他知道的、能够提供的这些东西实在让人震惊！我知道，我的一切将因此彻底改变！”这个记者事后是这样回忆的。[354]

就这样，斯诺登和波伊特拉斯建立起了联络热线，几乎每周都有邮件往来。在一封邮件里，斯诺登要她去找格林沃德，他希望两位记者合作完成这件大事。[276]于是，波伊特拉斯给格林沃德发出了一封邮件，里面写道：“本周你会在美国吗？我想跟你商量点儿事，不过最好面谈。”[358]

真是巧合，收到这封邮件的时候，格林沃德乘坐的飞机刚刚降落在纽约肯尼迪机场。见面后，波伊特拉斯非常紧张，也非常警惕，她要求格林沃德取出手机电池而不仅仅是关掉手机。格林沃德曾经听说过手机即使关机也有可能被悄悄激活，但这次从波伊特拉斯口中听到此话，他不敢怠慢，可没想到自己的手机电池居然取不下来，于是他专门把手机放回住处，然后返回会面地点继续商谈。[358]

波伊特拉斯告诉格林沃德，自己收到了若干封匿名的电子邮件，发件人态度诚恳，说是手里有些绝密文件，可以证明美国政府正在进行庞大的监视计划。等到看完波伊特拉斯打印出来的部分邮件内容，格林沃德告诉他的这位伙伴：

看来确有其人。我不知该怎样准确解释，却本能地感觉出这绝非戏言，此人的身份应该真实可信。[358]

除了他们俩，斯诺登的名单上还有一位。他叫巴顿·戈尔曼（Barton Gellman），原本是《华盛顿邮报》的记者，曾经多次获得普利策奖，后来转到《时代》周刊工作。戈尔曼写过一本书，题为“垂钓者”。“垂钓者”是美国前副总统切尼当年的一个代号。戈尔曼在书里讲述了这位美国历史上最有权力的副总统的历历往事，第六章“国外和国内的敌人”讲到切尼在“9·11”事件之后推波助澜，力主国安局实施“星风”行动计划。斯诺登反复阅读过这一部分内容，其中提到：

美国政府正在大规模搜查美国公民在自己的国家发出的电子邮件和传真，以及打出的电话……类似于通话记录和电子邮件标题这样的数据，都被数以十亿计地搜罗……分析人员很少能从中发现与恐怖威胁有哪怕一点点关联的信息。[110, 361]

戈尔曼的这些话正中斯诺登下怀。他请波伊特拉斯牵线，最终在5月16日联系上了戈尔曼。[362]

第二天恰巧是周末，米尔斯打算和朋友们乘船出海玩一周。斯诺登告诉她，自己也要出差，她从海上回来的时候自己很可能还没回来。[279]这是斯诺登能够设想的两人分别的最好方式，他已经准备就绪，一箭既发、再不回头。

我笃信某样东西，我愿意把我的生命投入烈火，燃为灰烬，落入尘土。[15]

接下来，斯诺登说自己要治疗癫痫，向主管请了病假，整理好行李，包括若干装有敏感文件资料的重要U盘，以及4台不同用途的新笔记本电脑，离开夏威夷飞抵香港。[276]一场惊天大戏就此拉开帷幕。

这一天是2013年5月20日，他到新单位工作还不足三个月。

到香港后，斯诺登马上就和波伊特拉斯联系，问她能不能到香港来见面。他还告诉她，自己已经和戈尔曼联系上了。波伊特拉斯随后用加密的“无痕迹”（OTR）聊天程序联系了格林沃德，问他愿不愿意陪她去一趟香港，并且想请他立刻和那个匿名知情人直接交流。没过一个小时，格林沃德就收到对方发来的电子邮件，稍后，两个人就用“无痕迹”程序聊了起来。神秘人告诉格林沃德：

我本想请其他人报道“棱镜”计划，让你专注于揭露更宽泛的内容，特别是美国国内的大规模监听行动，但现在我更倾向于让你来报道此事。我读你的文章已颇有时日，深知你做此事定会义无反顾，勇往直前……你的首要任务是亲赴香港。[358]

神秘人一遍又一遍地强调：马上来香港！马上来香港！

到这个时候，格林沃德还不知道波伊特拉斯介绍的这个知情人和曾经跟自己联系过的“辛辛纳图斯”就是同一个人，因为斯诺登这次使用了

另外一个电子邮件账户跟他们联系。这个账户叫作“Verax”。没想到，斯诺登这样一个“80后”极客竟还懂得一些拉丁语。

“Verax”这个单词在拉丁语中的意思是：说出真相的人。

第五回 说出真相

2013年5月24日，斯诺登再次和戈尔曼取得联系，希望对方保证《华盛顿邮报》把他提供的“棱镜”计划材料全文刊登出来。这对记者而言是一道难题，戈尔曼把它比作“炸弹”。斯诺登甚至给出了一个时间上限：72小时。这件事情戈尔曼显然办不到，他只能如实告诉斯诺登，自己无法保证报纸刊登什么内容，也无法保证他们选择什么时间刊登出来。[362]斯诺登想必非常失望。其实这一次他犯了一个非常幼稚的常识性错误，从某种意义上讲，他并不了解戈尔曼。他曾经对戈尔曼说：

你保护不了我，但是如果你能帮助我把真相说出来，我就认为这是一个公平的交易……没有人能拯救我。[362]

斯诺登关注的是公布真相，为此哪怕牺牲自己。戈尔曼则问他，如果情报泄露出去，是不是会让美国的敌人从中受益。

看到自己的“72小时”计划根本无法实现，斯诺登把工作重点再次转向波伊特拉斯和格林沃德。

手拿魔方

在一次与“Verax”的在线聊天过程中，格林沃德表示，希望对方能够提供一些文件，以便他能在去香港之前，对即将被爆出的内容有个初步了解。安装了一系列软件之后，格林沃德终于建立起一个比较安全的网络环境。很快，“Verax”就发过来25份文件，格林沃德随手点开了一个。这是一份绝密文件，是国安局内部使用的培训手册，详细讲解了各种最新的监控手段。他不由得心跳加快，因为在国安局历史上，如此重要的文件还没有被泄露过，而自己竟一下子就掌握了几十份这样的文件。他再打开另一份文件，标题是“棱镜”，这是一份幻灯片，同样是绝密级的。格林沃德再也不能抑制自己激动的情绪，他实在读不下去了。他想以最快的速度赶赴香港，而且此时此刻，他做出了一个非常重要的决定：让《卫报》加入进来。[363]

格林沃德生性好辩。他从小就以做过市议员的祖父为榜样，曾经以高中生的身份参加市议员竞选，尽管落败，却获得了精神胜利。1985年他进入乔治·华盛顿大学学习，大学期间曾因为不停地参与各类辩论而耽误了学习进度，用了5年时间才读完本科。接下来他以近乎完美的入学成绩考入了纽约大学法学院——这所法学院常年稳居美国法学院排行榜第6名。[364]毕业后格林沃德进入业内顶尖的沃利罗凯事务所工作，年薪20多万美元，但他很快就感到厌倦，并且离开了这家“全美最狠的法律事务所”，开设了自己的事务所。尽管几乎所有的大牌法律事务所都对格林沃德的小门面不屑一顾，但他的生意好得出奇。[365]

从事律师工作大约10年之后，格林沃德突然放弃了这一职业，转而开始了写作生涯。他建立了自己的博客网站，针对瓦莱丽·普莱姆（Valerie Plame）泄密案发表了长篇博文，从法律角度详细解构了对副总统国家安全事务助理刘易斯·利比（Lewis Libby）的各项指控，引起广泛关注。他言辞激烈、巧舌如簧，成为美国国家广播公司（MSNBC）的座上嘉宾，在电视上频频出镜，[365]同时他开始为网络杂志《沙龙》撰写专栏文章，5年后他离开《沙龙》加入《卫报》，经过协商，他从《卫报》那里获得了一项特权——完全的编辑自主权，也就是说，他的文章在发表前其他人不得对之进行编辑或者评论。他写好文章后，通过网络直接发表就可以。当然，如果他的文章可能给报社带来法律方

面的问题，则需要事先跟他们打个招呼、提个醒。[358]

格林沃德通过网络电话Skype和《卫报》美国分社主编简宁·吉布森（Janine Gibson）取得了联系。尽管已经从事高危的记者行业多年，格林沃德的保密意识仍然很弱。他刚开始汇报情况，就被吉布森就打断了。

吉布森：你是用什么方式打通我的电话的？

格林沃德：Skype。

吉布森：我认为我们不应该在电话上谈论此事，尤其不应该使用Skype。[353]

虽然格林沃德只说了几句话，吉布森已经隐约意识到他要说的事情非同一般，而且非常紧急。既然如此，她建议格林沃德立刻到纽约当面把情况说清楚。格林沃德连夜飞到纽约，和事先约好的波伊特拉斯会合。两人做的第一件事就是去买一台新的笔记本电脑，用这台从来没有上过互联网的笔记本作为工作用机，降低被监控的可能性。[353]考虑到格林沃德向来保密意识较弱，这多半是波伊特拉斯的主意。

《卫报》美国分社位于纽约百老汇大街536号6层，只有大约800平方米，面积不大，但现代化程度很高，完全是数字化的工作环境，总共仅有不到60个雇员，编辑人员只有31人。相比之下，他们的竞争对手《纽约时报》就像个庞然大物，仅新闻部就有超过1100人。[366-368]2007年，《卫报》曾经试图进入美国市场，但并没有明确的读者群，更不清楚读者想看什么。如此鲁莽的试探，两年后就毫不意外地以失败告终。[369]2011年，报社再次集结力量登陆美国，这一次他们派来了吉布森，目标非常明确：制作一份完全美国化的、电子版的《卫报》。和《纽约时报》《华盛顿邮报》这样的美国主流媒体相比，来自英国的《卫报》完全是一个无足轻重的“小人物”——尽管他们拥有世界第三大新闻网站。据说，2012年白宫举办新闻界招待会，《卫报》美国分社只得到两张入场券，座位还紧挨着卫生间和服务台。[367]报社虽雇用了不少当地人，特别是年轻人作为工作人员，但核心团队成员仍然是英国人，他们办的美国版报纸也仍然保持着自己的“英国风格”：面对每个月大约1000万的访问者，他们的网站会弹出一个问候窗口，上面清楚地显示着伦敦的天气情况。[369]

格林沃德和波伊特拉斯一起来到《卫报》美国分社，吉布森已经在办公室里等着他们了。格林沃德在笔记本电脑上打开了“Verax”提供的文件，吉布森马上就读了起来，脸上的神情显得越来越震惊。看完材料，吉布森正式决定参与进来。她让格林沃德第二天就动身，格林沃德非常高兴，但吉布森接下来的一个决定却让他有些不快：吉布森安排《卫报》资深记者埃文·麦卡斯基尔（Ewen MacAskill）一同飞往香港。这一突如其来的变化让波伊特拉斯非常恼火，因为事先只有她和格林沃德跟“Verax”联系过，她说：

不行，绝对不行。我们不能在最后时刻增加新面孔，而且我根本不认识他，有谁审查过他的情况？[353]

格林沃德只能好言相劝，自己到《卫报》不过几个月，对同事们并不熟悉，更谈不上信赖。派一个老员工一同前往，多半是为了能在关键时刻更好地掌控情况、把握方向。当然，吉布森派麦卡斯基尔“陪同”可能另有原因：相对于另外两位，他对香港的情况比较熟悉，早年他曾经在《中国日报》工作过，笔名是“袁麦”（Yuan Mai），常驻北京，多次到香港出差。在他的记忆里，那个时候在中国内地，“人们都骑自行车，穿着毛式中山装”。1996年，麦卡斯基尔进入《卫报》工作。[361]这次他陪着格林沃德他们去香港，也算是故地重游。

6月2日，格林沃德一行三人抵达香港。第二天一早，格林沃德就和波伊特拉斯来到事先约定的接头地点。安全起见，斯诺登专门设计了接头暗号和接头程序，还安排了两个见面时间：上午10点和10点20分。两个人首先要问指定房间附近遇到的第一个服务员，是否有餐厅可以用餐。这是接头的第一步。在附近监听的斯诺登会把这个当作一个信号。然后两个人要进入指定的房间，在一个装饰着巨型鳄鱼的沙发上等候，这是第二步。由于格林沃德和波伊特拉斯来得太早，他们没有见到接头人，等了5分钟后便起身离开，在一旁等待第二个见面时间的到来。10点20分，两人准时到达指定房间，坐在指定的沙发上等待。两分钟后，有人走了进来，手里摆弄着魔方——这也是事先安排好的接头细节之一。一切都像谍战电影的情节。两个人说着一些平常的话，其实是在对接头暗号。

格林沃德：餐厅几点开始营业？

斯诺登：12点。但是别去那儿，那儿的食物糟透了。[370]

格林沃德曾经问过，两人都没见过对方，怎么知道来人就是接头人。波伊特拉斯回答说，他会拿一个魔方。听到这话，格林沃德忍不住大笑起来，他觉得即将发生的一幕根本就是一部以香港为背景的跨国电影里的场景，怪异而荒诞。[276]其实，这个魔方已经陪伴斯诺登一段时间了。据他在夏威夷的同事回忆，他们经常看到斯诺登在办公大厅里走来走去，手里拿着一个魔方，不时在同事的办公桌上悄悄留下一点儿小礼物。[278]

等见到“Verax”本人，焦急等待的格林沃德和波伊特拉斯都吃了一惊：眼前的这个人太年轻了。虽然未曾谋面，但在格林沃德的想象中，这个神秘人应该50岁出头，见多识广、精明老道，准备牺牲自己向世人揭露真相，而要做出这样的决定，他应该经过很多年甚至几十年的磨炼和磨难，梦想才会彻底破灭。但实际上，眼前的这个小伙子看上去最多二十五六岁，身穿牛仔裤和已经有些褪色的T恤，戴着有些呆板的黑框眼镜，身体瘦削，脸色苍白，但非常警觉。[276]格林沃德心里顿时咯噔了一下：这次可能白来了。[371]波伊特拉斯后来是这样回忆的：

我一下子没了主意。我曾以为自己在和一个很高层次的人打交道，他应该年龄不小。我和他已经交往了一段时间，知道他在计算机系统方面的知识极为渊博，所以我又觉得他应该年轻些。总之我想他应该40来岁……[354]

斯诺登感觉到了那两个人的情绪变化，其实他也有些不太高兴，因为两个记者并没有严格按照约定的时间出现，这导致接头的验证过程变得复杂。[354]“跟我来！”斯诺登的话仿佛一道命令，格林沃德他们就跟着他，在这座酒店里转来转去，换了若干部电梯，最后进入了1014房间。房间很小很凌乱。刚坐下来，斯诺登就开始询问两人的手机情况。等到他们取下手机电池，把手机放进冰箱，斯诺登又从床上拿了几个枕头堵住了门缝。这一切安全措施都做完后，对斯诺登的采访才正式开始。刚才的些许不愉快很快就烟消云散。格林沃德发挥了他做律师时获得的工作经验，用类似取证的方式方法，对面前这个年轻人进行了长时间的询问，询问的目的就是想揭穿谎言、获取真相。他有各种各样的办法，比如连珠炮似的发问，给对方造成巨大的心理压力，从而得到真实的回答。再有就是针对相同问题，在不同语境下从不同角度发问，检验对方话语的真实性。在格林沃德面前，斯诺登表现得富有理性，思考问题有条不紊，回答问题简明扼要。[276]

除了斯诺登的成长过程、工作经历，格林沃德特别想搞清的一个问题是，到底是什么东西驱使他放弃事业，冒着成为重罪犯人的危险，违背保密和忠诚的要求把这些秘密泄露出来。斯诺登的回答是，世人有权知道自己的隐私遭到侵犯；面对恶行发生，他有道义和责任站出来发出反对的声音；当自己珍视的价值观受到威胁，如果保持沉默，他的良知将会受到拷问。他还特别提到了电子游戏对自己的影响：

游戏的主人公往往是一个普通人，他要面对巨大的邪恶力量，此时，他或者因恐惧而逃走，或者为信念而战斗。历史同样证明，只要对正义抱有坚定信念，即使是那些看上去普普通通的人，也能战胜最可怕的敌人。[276]

对斯诺登的世界观产生重大影响的还有互联网。对他们这一代人而言，互联网不仅仅是一个工具，它简直就是与现实生活平行的另一个世界。他说：

互联网让我体验了作为一个人可以享受到的自由，也开发了我的全部潜能……对许多年轻人而言，互联网是自我实现的一种途径，他们可以搞清楚自己是什么人，也可以想明白自己想成为什么人，但要做到这些，我们必须保护隐私、保持匿名，即使犯错也可能不会被追究。我很担心，我们这一代将是享受这种自由的最后一代人……我不想生活在没有隐私、没有自由的世界里，我不想让互联网的独特价值被人毁掉。[276]

从采访过程伊始，波伊特拉斯就进行了录音录像。这次采访前后经历了大约5个小时。其间斯诺登还提到，如果想把他掌握的大量文件在网上曝光，他自己就可以做，之所以找到格林沃德和新闻媒体，除了自己可以得到更多的法律保护，公众也可以通过阅读带有背景的文章，更加有条理、更加理性地理解被曝光的这些材料所包含的主要内容，以及曝光它们的重大意义。

格林沃德和波伊特拉斯并没有告诉斯诺登，《卫报》还派了一个记者和他们一起来香港。所以第一次和斯诺登见面，麦卡斯基尔并没有跟着去，而是一个人跑到香港岛，忙里偷闲、潇潇洒洒玩了一整天。[361]

傍晚时分，格林沃德他们回到了自己的住处。仍旧处于兴奋状态的格林沃德思如泉涌，连夜草拟了四篇文稿，每篇稿件都以一份高度机密

的政府文件为主题——这些文件都是斯诺登提供的。第一篇文章的主题是外国情报监视法庭的一道指令，命令威瑞森公司向美国政府提交公司掌握的所有国内通话记录。需要说明的是，威瑞森是美国最大的电信运营商之一，2013年4月公司在发布的报告中称，他们拥有1000万条通信线路，用户数超过1.2亿。[372]第二篇文章的主题是国安局总监察官2009年撰写的一份报告，这份报告彻底揭开了有关“星风”行动的各种谜团，这个曾经高度机密的行动计划终于大白于天下。前面介绍“星风”行动的时候，许多地方都参考了这份报告。第三篇文章讲的是一种名叫“无界线人”的监控工具。放在最后的第四篇讲的是后来最具轰动效应的“棱镜”计划。

和他一样加班加点准备稿件的还有麦卡斯基尔。格林沃德在自己的笔记本电脑上写好内容，马上用U盘拷给麦卡斯基尔。麦卡斯基尔在自己的电脑上修改好之后，再用U盘转给格林沃德。两个人几乎忘记了时间。年过六旬的麦卡斯基尔在体力上到底拼不过40多岁的格林沃德，他要起身去小睡一会儿，格林沃德还在那儿伏案写作。[361]

无论如何，格林沃德的写作速度着实令人称奇、赞叹和羡慕。[276]要知道，从纽约登上飞机开始，到这个晚上结束，格林沃德只睡了几个小时。在登机之前，波伊特拉斯交给他一个U盘，里面是斯诺登传给她的所有文件资料。飞机一起飞，他就开始打开那台没有上过网的新电脑、插上U盘，开始阅读。在16个小时的飞行时间里，他一边阅读文件，一边兴奋地做着笔记，几乎没有间断。[353]到了香港，难以抑制的兴奋再加上晨昏颠倒的时差问题，使得格林沃德只迷迷糊糊地睡了一两个小时。[276]即便如此，他依然能保持清醒的头脑和敏捷的才思，斯诺登后来也发现了这一点，他说：格林沃德让人印象特别深刻的一件事是，他能够彻夜不眠，连轴转好几天。[361]

格林沃德明白，斯诺登很快就不能像这样敞开心扉、发表言论了，留给自己的时间不多，他希望能尽可能多地和斯诺登一起，查看那些宝贵的文件。而且，他还知道，波伊特拉斯已经跟其他一些新闻单位和记者联系过，特别是曾经获得过普利策奖的戈尔曼，他也得到了斯诺登的一些文件，是自己眼前最强劲的竞争对手，一定要抢在他前面把新闻发出去。

争分夺秒

其实戈尔曼有他自己的苦衷。

戈尔曼曾在《华盛顿邮报》工作了20多年，2010年才跳槽去了《时代》周刊。这次得到斯诺登提供的文件之后，他跟老东家《华盛顿邮报》签订了一份协议，临时回去负责与这批文件有关的专题报道事项。

戈尔曼这样一种“临时工”的角色，和格林沃德在《卫报》扮演的角色，是不能相比的。他必须严格按照报纸的规矩办事，而格林沃德则拥有诸如完全编辑自主权这样非常特殊的权利。《华盛顿邮报》根本不可能马上就把斯诺登的文件报道出来，而是按部就班，一次又一次找来律师进行咨询。律师们提出了许许多多的要求，发出了各种各样危言耸听的警告。斯诺登曾经提出，让戈尔曼飞赴香港、与自己见面。针对这件事，《华盛顿邮报》聘请的律师们认为，从法律角度看，此举存在风险、并不理智。戈尔曼最终婉拒了斯诺登的邀请，没有前往香港和他见面。不仅如此，《华盛顿邮报》还劝告波伊特拉斯不要去香港，并且拒绝给她支付差旅费。

格林沃德已经准备好了稿件，他希望《卫报》立刻就能把它们刊登出来。但他的文章要发表必须征得主编同意。由于时差，他只能眼巴巴地等着吉布森主编上线。一看到吉布森即时聊天的状态变成了“在线”，格林沃德马上就给她发过去一条信息。他忙不迭地告诉主编，自己已经确证了斯诺登的身份和他提供的材料的真实性，并且已经写好了几篇文章。吉布森对有关威瑞森公司的那篇报道最感兴趣，但她告诉格林沃德，刊登这样涉及秘密文件的文章，需要提前将稿件传给政府——“向政府咨询”，这样就可以证明报社并没有危害国家安全的意图，也就可以避免被认为违反《反间谍法》而被追究刑事责任。《卫报》的律师们告诉她，这是一条不成文的规定。[276]

格林沃德询问主编，文章什么时候能发表。得到的回答是，还不确定，还需要跟律师再开一次会。格林沃德一下子焦躁起来。《卫报》会不会用几周时间跟政府谈判呢？他们会不会让《华盛顿邮报》冲在前面，以求自保呢？实在有太多的未知需要面对。关键时刻，麦卡斯基尔

安慰他说，不用担心，《卫报》非常积极，报社总编阿兰·拉斯布里奇（Alan Rusbridger）对有关威瑞森公司的稿件也非常感兴趣，并且承诺肯定会发表这篇文章。[276]

第二天，格林沃德带着麦卡斯基尔去见斯诺登。在他的房间里，这位老记者用了差不多两个小时的时间盘问他，跟格林沃德在前一天提的问题几乎完全相同。为了证明自己的身份，斯诺登从手提箱里拿出了一摞材料：驾照、一个已经过期的外交护照、他的中情局工作证，以及他用过的其他一些政府单位的工作证件。[276]查证格林沃德的“神秘线人”是否确有其人，这是《卫报》交给麦卡斯基尔的主要任务。等三人离开斯诺登的房间，麦卡斯基尔对格林沃德他们两人说：

我现在完全相信他是货真价实的。没有丝毫的怀疑。我一回酒店就给拉斯布里奇打电话，告诉他，我们应该立刻把文章登出来。[276]

从这一刻起，格林沃德和波伊特拉斯颠覆了原先对麦卡斯基尔的看法，三个人之间彻底消除了误解，成为一个团结的集体、一个强大的团队。麦卡斯基尔首先向吉布森复命。他们之间的问答是这样的：

吉布森：吉尼斯黑啤酒怎么样？

麦拉斯基尔：吉尼斯黑啤酒不错。[279]

看不懂吧？为了保密，麦卡斯基尔和吉布森事先约定了一套暗语。这样的回答就是告诉分社主编：神秘线人货真价实。[305]

接下来，麦卡斯基尔拨通了报社总编拉斯布里奇的电话。总编告诉他们，美国分社还需要跟律师最后再开一次会，会后一定会发表文章。他还说，《卫报》不仅要成为第一家曝光威瑞森公司丑闻的报纸，还要赶在《华盛顿邮报》之前，成为第一家曝光“棱镜”计划的报纸。[276]

拉斯布里奇的话没能让格林沃德安心太长时间。除了有关威瑞森的那篇稿件，“棱镜”计划的那篇文章几经修改也基本完成。想着自己手里有了两颗重磅炸弹，格林沃德的心里多少有些得意，但从波伊特拉斯口里得到的一个消息让他坐立不安：《华盛顿邮报》计划在周日，也就是6月9日刊登戈尔曼的文章。戈尔曼的这篇文章还将署上波伊特拉斯的名字。[276]性急的格林沃德感觉自己的耐心快要被消磨殆尽了。这也很可能是一种缺少睡眠的生理反应，人毕竟不是机器，严重缺觉后会异常

烦躁甚至情绪失控。

格林沃德又和吉布森联系了一次，并且甩下了狠话：他会尽一切可能保证文章即刻发表。大洋彼岸的吉布森则显得平静从容，她说：对于这一点，自己很清楚。她这样的态度，在格林沃德听起来，近似一种敷衍和应付，以至于他对《卫报》的信心都发生了动摇。他更加焦躁不安，四处联系熟人，准备候选方案。[276]

和格林沃德相比，吉布森颇有些大将风度。她制订出一个周密的计划，代号“凤凰传奇”。抽调骨干临时组成一个工作小组，在四楼的一间安全屋里集中办公，审查稿件、排版校对等。配套的保密措施非常严格：安全屋外有保安值班，只有少数几个可靠的记者可以进入。所有笔记本电脑都不允许接入互联网或者其他网络，保洁工也不能进去打扫卫生。几天下来，丢弃的三明治包装盒和用过的咖啡杯到处都是，这间安全屋简直成了一个垃圾堆。[373]

除了派格林沃德等三员大将远赴香港、获得第一手资料，吉布森还做了两件事：一是积极寻求法律方面的建议，避免触及红线；二是马上派专人前往华盛顿特区，与威瑞森公司和白宫接洽。[305]针对“向政府咨询”这样一个必要的环节，她给美国政府预留了三四个小时的反应时间。[305]

白宫方面的联系人名叫凯特琳·海顿（Caitlin Hayden）。就在6月5日这一天上午，白宫宣布苏珊·赖斯（Susan Rice）成为新一任国家安全事务助理，作为国家安全委员会的发言人，凯特琳·海顿忙得四脚朝天。尽管《卫报》发来的邮件里并没有直接透露具体的紧急内容，她还是抽出一些时间，在下午3点多给《卫报》代表回了一个电话，但听到的消息令她非常沮丧：《卫报》将在一个多小时之后，也就是当天下午4点30分，公开发表一篇文章，其中涉及外国情报监视法庭给威瑞森公司下达的一份绝密指令。凯特琳·海顿立刻跟吉布森联系，她竭尽全力，为政府争取到了一点时间：下午5点15分和《卫报》进行电话会议。[367]

白宫方面对此事高度重视，马上召集若干高级官员，谈判队伍成员相当有分量。这其中包括联邦调查局常务副局长肖恩·乔伊斯（Sean Joyce），国安局二号人物、常务副局长约翰·英格利斯（John Inglis）和国家情报总监办公室法务长罗伯茨·利特（Roberts Litt）。《卫报》方面只有两个人，美国分社主编吉布森和她的副手。[367]

谈判按时开始。会场气氛剑拔弩张。吉布森逐渐从随和活泼变得越来越刻板，她的英国口音也越来越明显。最终，白宫方面终于有人无法忍耐，大声吼道："你们没有必要公开此事！任何严肃的新闻机构都不会刊出此事！"[367]还有人说："你会发现，对于什么是国家安全，我们远比你们更有发言权！"吉布森一愣，马上冷冰冰地以牙还牙：

最最尊敬的先生们，我们发表什么内容，我们自己决定！……[367]我想你会发现，对于什么是新闻报道，我们远比你们更有发言权！[279]

最后，白宫方面表示，他们愿意就这个问题和报社的更高层负责人进行沟通。这是他们的最后一招。吉布森回答说，报社总编正在飞机上，无法跟他取得联系，她现在就是最终的决策者。[367]

此时此刻，吉布森承受着巨大的压力。面前是这帮气势汹汹的美国政府官员，身后则是步步紧逼的格林沃德。失去耐心的格林沃德甚至给她发来了"最后通牒"：

现在已经到了我给你的最后时限。如果再过30分钟还没有刊登稿件，我将终止与《卫报》的合作。[276]

就在点击"发送"之前，格林沃德稍微犹豫了一下，加上了下面这段话：

我明白，你有你的顾虑，必须做你认为正确的事情。但我要继续前行，做我认为需要做的事情。我很抱歉，没有办法两全其美。[276]

吉布森没有退路，只能一边竭力稳住急躁的格林沃德，一边安排人员赶紧完成最后的编辑、标题设计和排版工作。[276]

绝密法庭指令

2013年6月5日晚上7点，也就是吉布森和白宫方面的谈判结束一个小时之后，美国版《卫报》网站上终于登出了格林沃德撰写的第一篇文章，此时距离格林沃德一行到香港不过72小时。

美国国安局每天搜集数百万威瑞森公司用户的电话记录

独家专稿：绝密法庭指令要求威瑞森呈交所有通话数据，凸显奥巴马政府国内监视范围之大

4月发出的一份绝密法庭指令显示，美国国家安全局正在搜集美国最大的电信商之一、威瑞森公司数百万用户的通话记录。

《卫报》得到该法令的一个拷贝，其中明确要求威瑞森公司“不间断地”将其系统中“每一天的”所有通话记录都交给国安局，不论这些通话是在美国人之间进行，还是在美国人与外国人之间进行。

这份文件首次显示出，奥巴马政府不加区别地批量搜集数百万美国公民的通话记录，不论他们是否被怀疑做过任何错事。

秘密的外国情报监视法庭于4月25日通过联调局发布了该指令，授予政府部门毫无限制地获取数据的权力，为期3个月，有效期到7月19日。[374]

除了格林沃德的这篇文章，《卫报》还把法庭密令的全文发布在他们的网站上，全世界的好事者们终于有机会“围观”这篇难得一见的“奇文”，文中写道：

兹命令：记录保管人在命令有效期内必须每天向国安局提交下列物项之电子拷贝：（1）威瑞森公司提供的美国与其他国家和地区之间国际长途的所有通话详细记录或通话元数据；（2）威瑞森公司提供的美国境内所有通话详细记录或通话元数据。本指令不要求威瑞森公司提供完全在美国境外打入打出的通话元数据。

通话元数据包括综合通话常规信息，包括但不限于下列信息：会话

识别数据[例如，通话双方的号码、移动用户国际识别码（IMSI）、移动设备国际识别码（IMEI）]、中继线标识符、电话卡号、每次通话的时间及时长。

美国原本有三家主要的通信公司，只要控制了它们，几乎就可以控制全美的国内电话。这三家公司就是美国电话电报公司、微通公司和斯普林特公司。微通公司在2006年被威瑞森公司收购，成为威瑞森旗下的“商务网络服务公司”。也就是说，威瑞森公司代替微通公司，成为美国国内提供电话服务的最重要的公司之一。事实上，斯诺登这次提供给《卫报》的法庭指令针对的正是这家“商务网络服务公司”，也就是原来的微通公司。

曝光美国政府要求威瑞森公司提供通信数据的法庭密令，立刻在全球范围内引起强烈反响，几乎所有美国国内媒体的头条都跟风报道了这件事情，许多媒体要求采访格林沃德。这位原本就有些名气的记者一下子被推上风口浪尖。他利用媒体采访的间歇，再次去见了斯诺登。推开房门，他看到斯诺登正在收看美国有线电视新闻网的节目，嘉宾们热烈地讨论着国安局毫无节制的监视问题。[276]斯诺登曾经告诉过格林沃德，他最担心的，或者说唯一担心的一件事就是，自己的所作所为最后一无所获。格林沃德安慰他，结局不会如此。不过，其实格林沃德自己说这句话的时候也没有太大把握。[353]

多年来，格林沃德一直关注国安局滥用权力的问题，但他的感觉是，普通民众很难关注政府机构的监视行为。侵犯隐私和滥用权力对他们来说，过于抽象，他们很难真正理解这类事情的严重性和恶劣性，往往会轻描淡写地说，“这件事我们知道，但我们不在乎”。现在看来，他和斯诺登确实有点儿多虑了。

面对铺天盖地的新闻报道，白宫方面反应迅速，他们立刻对大规模收集通信数据的行为进行了辩解：

（《卫报》曝光的）这个指令并没有允许政府监听任何一个人的电话。政府获得的信息只涉及类似电话号码、通话长度这样的元数据，并不包含通话人姓名和通话的内容。

《卫报》刊登的这篇文章里描述的这些信息可以帮助反恐人员发现那些已被确认或者正被怀疑的恐怖分子，调查他们是否和其他参与恐怖

活动的人员，特别是居住在美国的这些人员联络。因此，这些信息对于保护美国免受恐怖威胁至关重要。[375]

不难看出，他们的主要方法还是那一条：尽量往“反恐”这个主题上靠。这是他们将所作所为合理化、合法化的最后一道“护身符”。只要能戴上这道“护身符”，就能安全过关。

美国参议院情报委员会主席、民主党人戴安娜·菲因斯坦（Dianne Feinstein）站出来替政府背书。她说：

据我所知，这个指令三个月一续，过去七年一直如此。外国情报监视法庭根据《美国爱国者法案》对业务数据的有关规定签发和延续这个指令。有关情况已经向国会汇报过，因此它是合法的。[372]

菲因斯坦试图从法律依据这个角度为威瑞森公司的法庭指令寻找一个说法。前面曾经详细介绍过“星风”行动，这里再简要回顾一下。从2006年5月开始签发电话元数据法庭指令，到2007年1月开始签发互联网内容和电话内容法庭指令，“星风”行动完成了其“合法化”的进程，政府方面甚至宣布“星风”行动到此为止了——他们只是玩了一个文字游戏。的确，以总统指令为依据、大规模搜集通信数据的“总统监视计划”结束了；但是，以法庭指令为依据、大规模搜集内容数据和元数据的有关工作一直按部就班地进行着，几乎一天都没有停止过，搜集到的各种数据和“总统监视行动”一样，仍旧归入“星风”专案——“星风”行动仍然在路上。

菲因斯坦提到了“有关情况已经向国会汇报过”。同样是民主党人的众议员洛夫格伦（Zoe Lofgien）却说：国安局提交给国会的电话记录搜集工作的年度报告总共不过一页纸，大概也就八段话。这样一种形式大于内容的汇报也就是走走过场，国会的监管多半是有名无实的。[376]

现在看来，“过去7年一直如此”的确不是虚言，不过菲因斯坦的这一番话其实是越抹越黑，一下子就把有关威瑞森公司的法庭指令和当年的“总统监视计划”“反恐监视计划”以及“星风”行动联系到了一起。由此可以有把握地推断，除了威瑞森，美国电话电报公司和斯普林特公司这两家通信巨头也会定期收到类似的法庭指令。据熟悉国安局内情的人士透露，实际情况正是如此。[377]而菲因斯坦把这样的法庭指令和《美国爱国者法案》捆绑到了一起，就连这个法案当年的起草人之一、众议

员小弗兰克·森森布伦纳（Frank Sensenbrenner,Jr.）也提出质疑：

我不相信，外国情报监视法庭签发的这样一种宽泛的指令符合《美国爱国者法案》的要求。不分青红皂白抓取几百万民众的通话记录是过分的、非美国式的。[372]

长期关注美国政府监视行为的参议员罗纳德·怀登和马克·尤德尔更是先后发表了明显带有警告性的声明，他们俩都是参议院情报委员会委员。怀登说：

参议院的规定禁止我在这个时候对一些细节进行评论，但是我相信，守法的美国人和他们的朋友打电话，他们跟谁打、什么时候打、从哪里打都是隐私……搜集每个美国人每天打出的每个电话的相关数据，是对美国人民隐私的严重侵犯。[372]

尤德尔则在声明中指出：

尽管我不能核实这篇报道的具体细节，但这样一种大范围的监视着实应该引起我们所有人的关注。美国人民应该对政府的这种越界行为感到震惊。[375]

面对如潮的报道、评论甚至批评，政府方面的种种说辞显得苍白无力，威瑞森公司则一言不发。依据这个法庭指令，公司被禁止向外界透露给联调局和国安局提供数据的有关情况。因此，这个指令同时也是一道“封口令”——他们被禁言了。[378]

有些媒体还向美国其他几家主要的通信服务商质询，是否也曾接到过类似的法庭密令。斯普林特、T-Mobile和世纪电信等公司都拒绝回答。[379]特别值得注意的是，他们并没有坚决否认此事。有专业人士指出，如果威瑞森公司被迫提供它9800万移动用户和210万固话用户的数据，那就可以比较有把握地推测其他公司也是如此。[378]因此，曝光针对威瑞森公司的法庭指令无疑将成为推倒第一张多米诺骨牌的最佳选择，极具轰动性和连锁效应。很可能正是这个原因，让《卫报》美国分社主编吉布森和报社总编拉斯布里奇一致看好格林沃德的这篇文章，极力促成这篇文章尽早发表。

说到这里，有必要对这些电话元数据法庭指令背后的“法律依据”稍微做一点儿解释。前文曾经提过，《美国爱国者法案》第215条对应

《美国法典》的第50卷第1861章，对《外国情报监视法案》第501条进行了修正。其中规定，政府可以获得各公司的“业务活动记录”，只要这些记录被认为与国家安全有关就可以。美国政府的法律“专家”把通信公司手中掌握的用户通信“元数据”解释为某种“商业活动记录”，因此认定政府部门可以要求公司提供这些数据。国安局的海顿局长后来把依据第215条的这样一种解释而开展的大规模监视行动称为“215计划”，这也成为“总统监视计划”，也就是“星风”行动的一个别名。[13]

怀登和尤德尔在若干年前就曾发出过警告，政府部门想出了一种说法，在《美国爱国者法案》中找到了“依据”，可以大规模地搜集美国国内的通信数据，而普通人并不能从法律条文中看出这一点，因而也就无法知道政府利用这部法律实际做了些什么。怀登说：

一旦美国人民发现，他们的政府对《美国爱国者法案》的秘密解释是这样的，他们必定会震惊并且愤怒。[380]

但由于涉及国家秘密，怀登他们无法在媒体上披露细节，只能语焉不详、旁敲侧击地说上几句。他们还曾经要求司法部部长把政府部门对《美国爱国者法案》的秘密解释公之于众，但他们的这个提案没能通过。[381]这次《卫报》曝光威瑞森公司的法庭指令之后，怀登承认，过去他们担忧的正是这件事情。[379]

可以长出一口气的还有当年在参议院投出唯一一张反对票的前参议员菲因高德，压在他心头多年的秘密终于大白于天下。早在2009年《美国爱国者法案》再次获得授权的听证会上，他就曾经做出过这样的声明：

我也是情报委员会成员。我想起在2005年辩论的时候，第215条的支持者们宣称，这些权力从未被滥用过。他们今天不能再这样说了，这些权力的确被滥用过。在此我不便细述。我建议各位议员在保密的情况下去了解更多信息……有关《美国爱国者法案》实施的关键信息仍处于保密状态，对此我非常担心……我认为美国国会和美国人民应当知道，第215条是如何被使用的。非常不幸的是，（因为信息涉密，）我们今天无法讨论这件事情。[382, 383]

在得知有关威瑞森公司的法庭指令曝光之后，菲因高德说：

我希望今天的新闻可以重启一场严肃的对话，即如何在保卫这个国

家的同时确保守法美国人的权利不受侵害。[384]

可以说，在斯诺登事件的这个回合中，媒体方面完胜。在历史上，媒体与美国政府间的角力曾经发生过多次，但很多时候获胜方并非媒体。就拿上一次曝光“星风”行动来说吧，过程就非常曲折、充满艰辛。

主编的决定

2004年是美国的大选年。共和党候选人是当时的总统小布什，他的竞争对手是民主党候选人约翰·克里（John Kerry）。这年夏天，“9·11”事件委员会终于正式发布了他们的调查报告。选择在这个时间发布也许只是巧合，但也有可能是提前安排好的——仿佛在提醒选民，“9·11”事件给美国带来极大的灾难，这几年，是谁辛辛苦苦带领大家挺过来的。这份报告对小布什来说，肯定是件利好的事情。转眼到了秋天，有关他早年服兵役时的负面往事被人扒了出来，这就不太妙了。随着最后的投票时间越来越近，竞选形势变得愈加激烈。

就在此时，《纽约时报》告诉白宫一个消息，他们准备发表一篇文章，曝光政府在“9·11”事件后授权国安局，在未得到法庭调查令许可的情况下，对打入美国的外国电话进行监视。[385]现在回过头再看，这篇文章的主题就是“星风”行动。由于行动计划的知情范围被严格控制，爆料人了解到的、提供给报社的只是这个行动中非常有限的一部分内容。当时只有极少数的几个人确切知道行动计划的正式代号（“星风”）和正式名称（“总统监视计划”），更不用说行动计划的全部内容了。政府内部的工作人员谈到“星风”行动的时候，通常都用“那个计划”来代称。前文提到波伊特拉斯曾借用这个名称，作为她拍摄的“星风”行动记录短片的标题。

在这次总统大选初期进行过一次民意调查，结果显示，小布什以54%的支持率遥遥领先，可以说是胜券在握。可就在9月底第一次公开辩论之后，形势发生了逆转，克里的民意支持率反超小布什。[386]不难想象，在这个节骨眼上，《纽约时报》如果把这样一篇负面文章发表出来，将会对选情造成什么样的影响。

美国新闻媒体要发表类似的曝光文章必须“向政府咨询”，证明自己并没有危害国家安全的意图，以避免法律方面的麻烦。菲利浦·陶布曼（Philip Taubman）当时任《纽约时报》驻华盛顿办事处主任，他奉命跟白宫和有关部门进行沟通。当时的国安局局长是海顿，他特意邀请陶布曼参观了国安局总部，希望他能认识到国安局的秘密计划都具有重大意义。陶布曼还拜访了国家安全事务助理赖斯，他们俩是20年的旧相识

了，就在不久前，陶布曼还在自己的住处隆重宴请过这位老朋友。[385]

谁也没想到，这一系列沟通的结果竟然是陶布曼自己转变了立场，变成政府的说客，反过来劝说报社总编比尔·凯勒（Bill Keller）不要发表这篇文章。凯勒本人后来也和海顿、赖斯等政府官员见了面。手里掌握着爆炸新闻的凯勒最终接受了政府方面的说法，接下来他做出了一个重要决定：把这篇文章扣压下来、不予发表。[385]

不过，这个决定最终成为凯勒先生最后悔的一件事情。人们一直很好奇，想知道凯勒做出这个决定的真正原因到底是什么。在不同场合、面对不同人，凯勒被无数次地问到这个问题。前前后后，他给出了多种不同甚至彼此矛盾的说法。有人问他，是不是因为他掌握了特别明确的证据，导致他决定扣压文章，他回答说没有。[385]凯勒反复强调，之所以这么做，是因为政府说有关方面都认为这个计划合法，发表这篇文章会让恐怖分子改变他们的行为习惯，使得追踪恐怖分子的任务更艰难。[387]后来，他又说自己当时并没有看出来这篇文章的主题是国安局计划的合法性问题，只是把它当作有关反恐问题的一般性文章，根本没有想到文章会成为有轰动效应的独家新闻。[385]当然，他还有更为冠冕堂皇的说法：

“9·11”事件刚过去三年，我们的国家还笼罩在巨大创伤的影响之中。我们，作为一家报纸，也不例外。这并不是爱国主义大泛滥，这是对当今世界依然危险的敏锐感受。[388]

相信在他的有生之年，凯勒还会不停地被追问，他的内心也会不停地被拷问。有人认为，凯勒的这一决定，最终帮助了小布什顺利连任，甚至可以说改变了美国的历史进程。对于这一点，凯勒自己也明白，要想彻底否认不大可能。[387]不过他说，自己评判是否刊发一篇文章，并不是看它会不会影响政局，而是看它是不是达到了报社的标准。[389]

世家子弟

说到《纽约时报》准备发表的文章内容，还要回到更早一点儿的2003年春天。那时，50多岁的托马斯·塔姆（Thomas Tamm）刚刚调入司法部情报政策审核办公室工作。塔姆一家在偌大的联调局里算得上声名显赫、非比寻常。塔姆的伯父爱德华·塔姆（Edward Tamm）是联调局早期历史上响当当的人物，是胡佛局长最重要的副手之一。抛开其他贡献不说，就连“联调局”这个名字，以及联调局“忠诚、勇敢、正直”的训示都源自他的手笔。塔姆的父亲奎恩·塔姆（Quinn Tamm）也曾是联调局的高级官员，一度做过胡佛的助理局长，还当过联调局犯罪实验室主任。塔姆的母亲是联调局鉴定部门的秘书，他的哥哥也曾在联调局工作多年。在联调局的某次庆典上，还在蹒跚学步的塔姆竟然进入胡佛的办公室爬来爬去。他还记得，8岁的时候，他和家人一起，站在胡佛办公室的阳台上，观看肯尼迪总统的就职典礼。简而言之，塔姆算得上联调局的世家子弟，“根红苗正”，非常可靠。[390]

塔姆从布朗大学和乔治敦大学法学院毕业后一直当律师，后来成为资深的审判庭律师，负责谋杀和绑架等刑事案件的诉讼事宜。据了解他的人说，塔姆非常善于跟陪审团沟通，特别擅长“讲故事”，再复杂的案情经过他的讲述都能变得很容易理解。2000年，由于工作出色，塔姆获得了司法部的最高荣誉——“约翰·马歇尔奖”。不过，颇受前任司法部部长珍妮特·雷诺（Janet Reno）赏识的塔姆却不受后来的阿什克罗夫特部长待见。[390]

司法部情报政策审核办公室最重要的一项工作是向外国情报监视法庭提出申请，对危及国家安全的恐怖分子或者间谍以及嫌疑人进行监视。塔姆调进这个办公室工作后不久，就发现了一个奇怪的现象：某些监视申请的处理过程非常特殊。这些特殊申请只能由司法部部长签字批准，然后直接递送监视法庭的首席法官。塔姆不知道为什么这些申请会如此特殊，需要绕开监视法庭的另外10位法官，就连通常情况下可以签署其他申请的常务副部长也被绕了过去。塔姆所能知道的就是这些申请都属于某个高度机密的行动，办公室里的其他人对此讳莫如深，但凡提到这个神秘的行动，都用“那个计划”来代称。[390]

办公室里专门有一个人负责查询国安局系统，看看监视申请是不是属于“那个计划”。比如，塔姆他们会问，“555–1212号是不是属于‘那个计划’？”一两天后，他们会得到一个结果。如果不属于，就按照正常程序逐级上报，否则就走特殊程序。5%～10%的申请属于“那个计划”。[391]

塔姆非常困惑，偏偏他又属于那种有点儿“较真”的人，他的儿子称之为“正义情结”。他看不出这些申请特殊在什么地方，因而实在想不通为什么要特殊处理。终于有一天，他找到顶头上司莉萨·法拉比（Lisa Farabee），要求对方给出一个解释。他的问题直截了当：“你知不知道‘那个计划’到底在干什么？”法拉比说：“这个问题，你压根儿就不该问。”停了停，她又加了一句：“我认为他们不合法。”塔姆觉得太不可思议了，自己是一个执法人员，怎么能去干违法的事情呢。[390]

后来他联系上了桑德拉·维金森（Sandra Wilkinson），她是自己多年前的一个同事，现在在参议院司法委员会工作。塔姆把自己对于“那个计划”的关切，以及情报政策审核办公室里的异常情况一五一十地告诉了维金森。他希望这位老同事去找找情报委员会，请他们出面调查这件事情。过了几周，塔姆再次把维金森约了出来，没想到对方反应非常冷淡，还让他别再折腾这件事了。接下来的一段时间，塔姆的内心备受煎熬。渐渐地，他下定决心通过媒体曝光此事。[390]

塔姆最初希望能联系上赫许，就是当年曝光过尼克松时期中情局黑幕的那位《纽约时报》的记者。可惜塔姆怎么也找不到他的联系方式。不过，他很快就注意到《纽约时报》曾刊登过若干篇有关司法部的重头文章，写文章的记者名叫埃瑞克·利希特布劳（Eric Lichtblau）。[390]

塔姆后来回忆说，搜索到利希特布劳的电话号码毫不费力，不过在鼓足勇气拨通电话的时候，他还是忍不住浑身发抖。在电话里，塔姆告诉该记者，自己名叫“马克”，曾经是司法部的雇员，有重要情况需要面谈。随后的几次见面，利希特布劳都带上了自己的搭档詹姆斯·瑞森（James Risen）。塔姆的真诚态度以及他内心的恐惧深深地感染了两位记者[390]——这种恐惧是每个爆料人都会经历的，因为他们面对的是强大的政府机器。

塔姆对“那个计划”的叙述听上去非常可信，但同时信息非常有限且非常含糊。[390]有关“那个计划”的更多细节，只能靠记者自己想办法去

弄清楚了。事实上，这两位记者陆陆续续通过其他渠道掌握了更多情况，利希特布劳主要是从司法部入手、瑞森则主要是以情报单位为突破口。[392]塔姆特别希望文章能够在大选前发表，让小布什政府倒台，可他没想到，瑞森和利希特布劳的这篇文章竟然搁浅了。

在《纽约时报》内部，瑞森素以脾气火爆和敢于犯上著称。他曾经写过一篇报道，强烈质疑政府发现的关于伊拉克大规模杀伤性武器的所谓证据。他的这篇报道与报社已经发表的另一篇报道针锋相对，也与当时的主流观点格格不入，文章于是被搁置不用。这一次，得知自己写的文章又遭遇波折，瑞森放下架子，在大选前一周给报社副总编吉尔·艾布拉姆森（Jill Abramson）打电话，请求她说服凯勒。结果却是，该报道不仅大选前没有发表、大选结果出来后也没有发表。这可把瑞森气坏了。从此以后，他再也不搭理艾布拉姆森和凯勒了。[385]

可贵的是瑞森并没有因为愤怒失去理智。他想出了一个办法：在自己新写的一本书里，以这篇文章为基础，写出了一章内容。他的这本新书名为“国家战争”（*State of War*），而这一章的标题就叫“那个计划”。凯勒得知了这个消息，马上改口说，上次成稿后，两位记者又夯实了证据、充实了内容，他们的文章可以马上发表。其实和一年前相比，文章的实质内容几乎没有变化，他的这套理由根本站不住脚。据了解内情的人说，刺激总编改变决定的直接动因就是瑞森的那本新书。说白了，凯勒必须抢在新书出版前发表这篇文章，因为他知道，如果这本书抢在《纽约时报》之前曝光“那个计划”，人们就会认为《纽约时报》实在是太糟糕了，那将成为报社的一场灾难。[393]

“向政府咨询”的过程即刻再次启动。没想到，时隔一年，白宫对这篇报道依然非常重视，政府与媒体间的角力依然惊险刺激。

2005年12月6日，小布什在自己的办公室亲自接见了《纽约时报》的主要人员。这是一种空前的会议规格，出席的有美国总统和他的法律顾问哈丽雅特·迈尔斯（Harriet Miers）、国家安全事务助理斯蒂芬·哈德利（Stephen Hadley），坐在他们对面的是报社的出版商阿瑟·苏兹伯格（Arthur Sulzberger）、凯勒和陶布曼。国安局局长海顿坐在一旁，在厚厚的本子上做笔记。[385]

会议持续了一个小时。总统最终亲自上阵。他说，如果报社曝光了这个秘密计划，而美国再一次遭受恐怖袭击，“你们的双手将沾满鲜

血”。也许正是因为政府这样一种赤裸裸的威胁，反倒激发了凯勒的血性。一走出白宫，他就忍不住对苏兹伯格说，他们所说的一切丝毫不能改变自己的想法。苏兹伯格连连点头称是。[385]

“反恐监视计划”

2005年12月16日，《纽约时报》发表了瑞森和利希特布劳的文章，指名道姓地对美国政府进行批评：

小布什批准，绕过法庭监听通话

据多位政府官员称，“9·11”事件发生后几个月，小布什总统秘密授权国家安全局在没有法庭调查令的情况下，对美国人以及在美国的外国人进行监听，寻找恐怖分子活动的证据，正常情况下对美国国内进行监听需要调查令。这些官员还说，根据2002年签署的一份总统令，为了追踪与“基地”组织联系的“可疑号码”，国安局未得到调查令许可，对美国境内数百人甚至数千人的国际电话和电子邮件信息进行了监视。该局还希望获得监视全部美国国内通信的调查令。[394]

小布什对于《纽约时报》发表这篇文章已经有所准备。第二天，他就发表声明，试图进行还击：

在我们的国家遭受恐怖袭击几周之后，我授权国家安全局对与“基地”组织和其他恐怖组织有联系的国际通信进行监听。这种授权符合美国法律和宪法的要求……

这是一个高度保密的计划，事关我们的国家安全。计划的目标是发现和阻止针对美国及其朋友和盟友的恐怖袭击。昨天，新闻机构在不正当地得到线索之后，在他们的媒体报道中暴露了这个秘密计划。我们的敌人因此得到了他们本不应该得到的信息……泄露保密信息是违法的，它提醒了我们的敌人、危害了我们的国家……

我授权的行动每隔大约45天就需要评估一次。我曾经30多次授权继续执行这个计划。我还将这样做下去，只要我们的国家还在面临“基地”组织或者其他恐怖组织的威胁。[395]

对于“那个计划”启动的准确时间，《纽约时报》的说法并不正确。小布什心里当然明白，于是在自己的声明里悄悄做了一点儿更正，从“‘9·11’事件发生后几个月”提前到“遭受恐怖袭击几周之后”。前面介

绍“星风”行动的时候曾经提过，小布什第一次签署命令授权行动开始的日期是2001年10月4日。

不过，小布什的这番说辞并不能服众。参议员菲因高德就说：没有哪个参议员或者众议员会同意，这样就能对国安局监听国内通信进行授权。怎样获得授权，法律上规定得清清楚楚。参议院司法委员会主席阿伦·斯柏克特（Arlen Specter）则表示：行政部门的此类行为不能原谅，他的委员会将立刻着手调查此事。[396]

小布什很快有了一个新的主意。2006年1月23日，他专门就反恐战争问题在堪萨斯州立大学做了一次演讲，演讲中他突然话锋一转，讲了下面一段话：

我想谈谈另一个计划……你们最近在新闻里了解到一些有关情况。我想把它称为“反恐监视计划”。敌人袭击了我们，我认识到大洋并不能保护我们，我就问那些为你们工作的人一个问题——他们也在为我工作：怎样利用信息最好地保护美国人民？……他们提出了一个计划……对从美国打到国外的某些电话进行监听，如果他们有理由怀疑其中一个号码与“基地”组织有关的话。[397]

到这个时候为止，“反恐”仍然是一个不容置疑、不能颠覆的大事，拿它作为名头给“那个计划”正名，无疑是一个非常“聪明”的办法。当然，小布什不可能完全忘记自己在2004年竞选期间说过的另外一番话：

无论什么时候美国政府考虑开展监听工作，它都首先需要法庭指令。当我们讨论追踪恐怖分子的时候，我们都会说，在开始追踪之前要获得法庭指令。[389]

看来，解决问题的关键点是“法庭指令”。在他说出这段话时，对监视行动进行授权的法庭指令针对的都是比较明确的目标。如果法庭指令能够突破这个局限，划定一个比较大的范围，针对一大批目标，他的这番话将仍然成立。一年之后，小布什通过《保护美国法案》做到了这一点。

除了揭露美国政府的“那个计划”，瑞森和利希布劳特还在他们的文章里埋下了这么一句话：“报社推迟了一年时间发表本文。”这句话立刻就被细心的记者们发现了，他们顺藤摸瓜，很快就把凯勒扣压文章前前后后的细节都曝光了出来。[398, 399]这一事件不仅影响到民众对凯勒

个人的看法，而且深刻地影响到他们对《纽约时报》的看法。报社里有人曾以为，两位记者的文章最终发表了，他们两人还因此获得了2006年的普利策奖，那么这一页历史很快就能翻过去。但直到10年后，想要说出真相的斯诺登仍对波伊特拉斯表示，他了解《纽约时报》的这段往事，也因此怀疑这家报社还会故伎重演，因而不愿把曝光黑幕的重任交给他们。[400]这就表明，在很多人眼里，《纽约时报》的这一页历史并没有彻底翻过去。[393]

2014年，最先曝光斯诺登事件的《卫报》和《华盛顿邮报》一同获得了普利策奖。凯勒没有想到，由于自己的决策，《纽约时报》10年前在与政府的一场角斗中输掉了，这一结果竟然导致10年后，报社同时输给了其在美国国内和海外两个最大的竞争对手。凯勒早已卸任，这样一种痛苦只能由《纽约时报》继任的总编们来承受了。[393]

斯诺登并非第一个拒绝跟《纽约时报》合作的爆料人。原本并没有《纽约时报》和《华盛顿邮报》出名的一些新闻媒体，也成为这些爆料人的新选择，比如《巴尔的摩太阳报》或者《今日美国》。[389]

一个好汉三个帮

托马斯·德雷克永远也不会忘记他第一天到国安局上班的情景。

按照要求，他在清晨5点就赶到了上司的办公室。这实在太早了，天还没亮，他记得非常清楚，当天的天气非常晴朗、空气非常清新。他的这位上司名叫莫琳·巴津斯基（Maureen Baginski），是信号情报分局的负责人，习惯于每天非常早就开始工作，所以也给德雷克提出这样一个“不近人情”的要求。前面曾经提过，海顿局长上任后，积极在国安局推行改革。德雷克和其他十多个人一起被局里聘为改革专员，而且他有一个听上去很漂亮的头衔，叫作“高级改革主管”。[11]据熟悉他的朋友说，德雷克对事情总有他独特的视角，他善于把外部世界最好的元素引入国安局这样一个大型单位封闭的思维模式里。[401]如此看来，把他聘为改革专员，算得上是物尽其用、人尽其才。

这段时间局里给德雷克布置的主要任务是让他紧紧跟在巴津斯基身后，全面了解她承担的各项职责、参加的各种会议以及参与协调的各项工作，为下一步的改革做准备。第一天上班，他的工作是跟着巴津斯基，在法律事务办公室，向参议院情报委员会的技术顾问小组进行汇报。汇报正在进行之时，巴津斯基的助理突然推门进来，告诉大家说有架飞机撞上了世界贸易中心双子塔中的一座高楼。没过多久，门再次被推开，这回的消息是双子塔中的另一座也被撞了。德雷克再也坐不住了，他一下子站了起来，大声说道：“美国遭到袭击了！”[11]

没错，这一天就是2001年9月11日，是德雷克到国安局上班的第一天。

进入国安局之前，德雷克曾经在国安局的若干家承包商那里工作过多年。更早的时候，他曾作为美国空军信号情报部门的密码专家，在间谍飞机上工作过，还曾在中情局干过一段时间。[401]恐怖袭击打乱了海顿设计的改革进程，也改变了德雷克的工作内容：他变成信号情报分局事实上的联络官。为了做好这项工作，他在其他团队的帮助下建起了一个网站，发布国安局各个部门的最新情况，全局都可以看到。[11]

“9·11”事件恐怖分子得逞，对整个美国情报界而言是一次巨大挫

败。对国安局而言也是一样：他们没能提前发出预警信号，更没能预先提供抓捕恐怖分子的线索。他们在这次恐怖袭击过程中所做的和普通美国人一样，通过电视获取“情报”，这不能不说是一种耻辱。作为当时美国情报界的最高首长，中央情报总监特内特发出了这样的号召：

你们的实验室里有什么、你们的单位里有什么，把它们统统拿出来，投入战斗！我们需要它们！我们要对付恐怖分子，它们有可能用得上！[11]

为了响应上级的号召，德雷克开始着手摸清局里正在开发的几十个系统，看看哪些能够派上用场。这其中就包括“细线”系统，这个名字在前文曾经提过。该系统包含十几个模块，前前后后曾投入过大约300万美元。从投资规模来看，实在不算很大。大部分开发工作由国安局内部的“信号情报自动化研究中心”完成，剩下的工作由少数几个合同商承担。[11]三年前，德雷克曾经作为合同商雇员，使用一种叫作“Jackpot”的软件，对“细线”系统的关键模块进行过代码性能分析。[12]也就是在那时，他认识了宾尼。

宾尼是国安局的元老，已经在这里工作了30多年。1992年前后，他和约翰·泰嘉特（John Taggart）一起组建了“信号情报自动化研究中心”。他们大概就是从这个时候开始着手建设“细线”系统的。泰嘉特负责系统前端，也就是数据采集部分，接收从电缆、卫星和光纤等各种信息源传来的数据。宾尼负责后端，对接收到的数据进行处理和分析。后来泰嘉特退休，爱德华·卢米斯（Edward Loomis）接替了他的位置。1997年，宾尼开始担任地缘政治分析部门的技术主管职务，这个部门规模很大，工作人员有6000多名。[12]

宾尼先后解决了“细线”系统里的密码问题和算法问题，除此之外，他还专门设计了一个加密过程：如果系统发现收集到的是美国人的数据，就会自动对这些数据进行加密。[402]这样就可以避免收集美国人的数据、侵犯他们隐私的嫌疑。2000年11月，“细线”系统完成了联调联试，宾尼他们打算再接再厉，在国安局更多的场所推广这个系统。两个月后，他们拿出了一个方案，计划在18个重要的反恐地点部署这个系统，经费总额达950万美元。他们从局里请来很多人评估这个推广方案。这些人很快就意识到，宾尼他们的方案与海顿局长正在启动的“开拓者”计划有很多内容交叉重叠，如果他们同意部署“细线”系统，则意味着国会可能根本没有必要再投资几十亿美元实施“开拓者”计划，而这是海

顿局长以及局里的那些人都不希望看到的。[11]于是，在恐怖袭击发生前一个月，“细线”系统被国安局“毙掉”了。[11]

在宾尼他们设置的18个场点里，有一个就是美国情报单位设在也门的安全屋。德雷克事后发现，这些安全屋曾经监听到了“基地”组织的电话。但令人惋惜的是，由于缺少必要的处理和分析工具，这些重要的信息并没有发挥作用，而是躺在数据库里，没有人知道。[11]

“9·11”事件之后，德雷克认为，为了响应特内特的号召，国安局应该尽快重新启动“细线”系统。德雷克从宾尼那里还了解到了这样一个情况：“那个计划”使用“主干道”的时候，去掉了保护美国人隐私的加密过程，也就是说，国安局正在把原本用于对外情报的技术手段，直接转用在了美国人身上。这让德雷克不寒而栗，因为他知道，国安局已经跟美国电话电报公司、斯普林特公司和微通公司等通信运营商联系过，可以大量使用它们的用户数据。[11]

事不宜迟。德雷克把宾尼等人提出的“细线”推广方案翻了出来，稍作修改，交给了巴津斯基。他不断地向自己的上司施压：

我们彻底违反了《外国情报监视法》，违反了《宪法第四修正案》，违反了美国宪法。我们在做什么？我们手里其实有解决方案。我们有。我们可以追踪恐怖威胁。这个方案可以提供非常好的情报，可以保护美国人民。[11]

面对德雷克的纠缠，巴津斯基唯一的办法是免战高悬、避而不见。她给德雷克留了一张纸条，上面写着：“他们已经有一个非同寻常的计划了。”[11]德雷克当时并不知道这个计划的真实名字，他所知道的是这个“非同寻常”的新计划并不打算启用“细线”系统的全部功能，它只使用了系统中一个叫作“主干道”的模块，利用这个模块“建立联系链”。当然，这个模块的算法也是宾尼设计的。

德雷克深知，有了通信运营商的“鼎力”支持，再加上去掉隐私保护的“主干道”模块，国安局将具有强大的数据获取和分析能力，美国人的个人隐私和通信安全将面临前所未有的威胁。他最后一次恳请巴津斯基考虑他的建议，女上司再一次拒绝了他：“你给法务长办公室打电话吧。”接电话的是国安局副法务长维托·波滕扎（Vito Potenza）。

波滕扎：你不明白。所有的律师都赞成它，它是合法的。白宫已经

授权国安局作为“那个计划”的执行单位。

德雷克：你是说，因为“9·11”事件，我们要抛弃《宪法》？

波滕扎：你不明白。我们现在处于紧急状态。为了应对威胁，必须采取非常特殊的办法。我们非常需要数据。[11]

“别再问更多的问题了，德雷克先生。”波滕扎用这句话结束了他们的对话。[11]

与此同时，宾尼那里正在发生翻天覆地的变化。先是进来了一大批设备，最初堆在地上，没几天，人们就在“自动化研究中心”的大厅里把这些设备组装起来。接下来，宾尼手下的承包商雇员大都被调到了一个新部门。[12]一天，有个熟悉宾尼的雇员找到他，对他说：

你知道吗，他们正在干的事是把所有国内数据都抓进来，这些数据是美国人在国内的通信记录，每天有上亿条，全都来自美国电话电报公司。[12]

这实在太让人震惊了！作为国安局里的老员工，宾尼意识到，离开国安局的时间到了，此地不值得留恋。他对自己的同事说：

这里变得太不正常了。它违背了所有东西，违背了这个国家的基本原则，违背了宪法，违背了无数的法律……显然，我再也不能为这里做任何事情了。[12]

2001年10月底，宾尼向局里递交了退休申请。和他同时申请退休的还有负责“细线”系统前端的卢米斯，以及资深分析员柯克·韦伯（Kirk Wiebe）。但对宾尼而言，这件事远没有结束。他找到了在众议院情报委员会工作多年的黛安娜·罗克（Diane Roark），向她反映情况。[12]

罗克长期与国安局联系紧密，对德雷克和宾尼等人也非常熟悉，更难得的是他们几个人对很多事情的观点相同，因此也就成了很要好的朋友。[401]罗克马上向众议院情报委员会领导汇报，但旋即她就看出来，这些领导早已知道“那个计划”。[12]他们让她去找国安局局长海顿。海顿的回答很明确、也很强硬：

对于我们正在做的这些事情，以及如何做这些事情，我们都非常骄傲。[401]

宾尼和罗克等人只好另想办法。几个人再次商量的结果是他们拐弯抹角给最高法院首席法官捎去了一封信，但却石沉大海，没有一点儿回音。[12]

宾尼又找到韦伯商议，向国防部总监察官反映情况。不过国防部总监察官主要负责调查国安局的欺诈、浪费、滥用职权和腐败情况，设立的举报热线不能用来反映涉及高度机密的非法国内监视问题，而只能用来举报不涉及任何秘密的问题。于是他们选择国安局在系统建设方面的不当行为作为突破口，主要内容是局领导放弃大有希望的“细线”系统、上马管理混乱的“开拓者”计划等。宾尼、韦伯、罗克和卢米斯在举报文件上签下了自己的名字。这些事情发生在2002年9月。[12]

国防部总监察官对他们反映的问题高度重视，历时两年多才完成全部调查工作，最后提交了一份长达100多页的报告。这份报告对国安局的杀伤力巨大，最终导致国会收回了国安局可独立签署大额合同的权力。

不过，宾尼他们关注的重点显然并不在此，他们又找到司法部总监察官，也是毫无结果。曝光国安局非法监视问题的道路依然漫长曲折，而仍在国安局工作的德雷克的处境越来越艰难。尽管参与起草了向国防部总监察官的举报文件，但考虑到自己还处在体制内，德雷克最终没有在文件上署名。[11]

2005年亚历山大局长上任，机会似乎来了。11月，德雷克交上去一份备忘录，算得上是给新局长的一剂猛药，备忘录的题目是“你所面临的形势”。结果出乎德雷克的预料：局里重新安排了他的工作，他仍然拥有一间自己的办公室，办公桌上继续插着国旗，说明他是局里的高级官员，除此之外再无其他配备，手底下既没有项目也没有人，什么都没有。面对这样一种结果，德雷克彻底失望了。[11]

德雷克后来说，自己跟西沃恩·高曼（Siobhan Gorman）联系，是罗克出的主意。不过，罗克对他的这种说法并不认可。高曼是《巴尔的摩太阳报》的女记者，经常报道有关美国情报界的一些事情。富有情报工作经验的德雷克非常谨慎，从不直接和她见面，而是采用加密邮件的方式与她通信，通过邮件先后传递给她一些国安局的非密文件。[401]

追查举报人

2005年12月，《纽约时报》刊登了瑞森和利希特布劳撰写的那篇重磅文章。半个月后，司法部开始调查到底是什么人向记者泄露了秘密。他们胜券在握，原因很简单，知道“那个计划”，也就是“星风”行动的人实在没有几个，掰着手指头都能数清楚。德雷克知道，他们用不了太长时间就会追查到自己身上，尽管他从未跟《纽约时报》的记者接触过，但自己经常在单位发表不同意见，肯定会被列为重点怀疑对象，进而调查者就肯定会发现自己跟高曼的关系。[11]

从2006年1月开始，高曼把《巴尔的摩太阳报》作为自己的阵地，针对国安局的假、丑、恶接连发表文章。第一篇题为“系统错误”，披露国安局的“开拓者”项目是一个典型的钓鱼工程，耗资巨大，进度一再拖延，要求悄悄降低，经费却不断上涨。[252]5月18日，根据德雷克提供的线索，高曼发表了另一篇重要文章，题为“国安局封杀过滤合法电话数据的系统”，文章从正面介绍了投资少、见效快的“细线”系统，处于反面的是混乱不堪、了无成果的“开拓者”项目，两相对比，一个天上、一个地下。除此之外，文章只是隐隐约约地提到国安局正在不加选择地搜集美国人的通信数据，但并没有花费太多笔墨。[261]

高曼的文章发表后不久，敏锐的德雷克就发现自己处于被全面跟踪和监视的境地。尽管搬了家，但自家门口总是停着几辆车，如影随形、摆脱不掉。根据自己在中情局工作的经验，德雷克当然知道这几辆车是做什么的，不过他并没有告诉自己的家人，而是选择一个人默默地承受、静静地等待。[11]

2007年7月，德雷克突然接到韦伯的电话。他担心的一切正在一步一步成为现实：宾尼、韦伯和罗克的家都被搜查了。4个月后的一个凌晨，德雷克透过窗户看到突然有很多车停在自家门前，从车上下来十多个联调局特工。他明白，这一天终于来了。[11]

从国安局“光荣”退休的宾尼家被搜查的经过，像是一部好莱坞动作片的场景。他的儿子一打开房门，特工们就冲了进来。正在淋浴的宾尼突然间看到乌黑的枪口对准自己，惊恐万分。[264]相比之下，对德雷

克的搜查就“文明”多了。但搜查之后，所有特工都很失望，他们的目标是找到这些国安局人员跟《纽约时报》记者联系的证据，结果一无所获。这句话并不准确，意外的惊喜还是有一点儿的，因为德雷克很快就坦白自己跟《巴尔的摩太阳报》的记者联系过。和搜查其他几个人家的结果类似，特工们把房间里的计算机、照片、有关的书籍，甚至德雷克撰写学位论文时整理的资料搜罗一空，算是对上面有个交代。[401]

被搜查的不仅是德雷克和他的三个好伙伴宾尼、韦伯和罗克，还捎带上了卢米斯。说起卢米斯，他被搜查多少有点儿“冤枉”，因为他一直都认为国安局当时进行的“那个计划”是合法的，而且认为自己始终是站在美国政府这一边的。也正是因为这样，他对自己被搜查这件事情怎么也想不通。他被搜查的理由其实很简单，他曾在举报信上签名。德雷克和他的伙伴们的家庭顺利渡过了这次难关，卢米斯的家庭却因此破裂，这让他的生活更加消沉、郁闷。[402]

也就在2007年8月，塔姆外出回家，看到自家门口停了一排汽车，路中间站着自己的律师，身穿蓝色外套的联调局特工抱着盒子从自己家里进进出出，里面装着所谓的证据。[391]他们满载而归，带走了塔姆和他的孩子们的笔记本电脑、他个人的文件和书籍。[390]更重要的是，向《纽约时报》记者爆料的线人浮出水面。但是，瑞森他们的那篇文章还涉及其他线人，对于这些人到底是谁，瑞森一直守口如瓶。到今天为止，这些“深喉”的具体身份依然是个秘密。

德雷克以及塔姆的这些遭遇陆陆续续都被媒体报道出来，这些文章斯诺登全都仔细读过。他一方面因为自己的爆料成功而感到高兴，另一方面开始为自己的女友和家人担心起来。尽管到这个时候为止，他还没有走到幕前，向大众公开自己的身份，但博艾汉公司已经把他列为失联人员，国安局随后展开了针对他的密集搜寻工作。[403]就在《卫报》登出格林沃德的第一篇文章的同一天，斯诺登在夏威夷原先租住过的房子门口出现了两位不速之客，其中一人还身着警服。当地一家房屋中介公司的雇员海姆正在屋中。两个陌生人询问她，原先租住在这里的人有什么异常、到哪里去了等问题，海姆当然一无所知，无法回答。[279]

2013年5月，由于房东打算把房子卖掉，斯诺登和他的女朋友不得不从租住的房子里搬出来，另找了一处地方居住。[404]斯诺登悄悄在房间里安装了一套远程监视设备，房间里的任何风吹草动他都能通过网络观察到。《卫报》关于威瑞森公司的报道一出，国安局很快就把斯诺

登作为首要嫌疑人，派两个人到他的住处了解情况。这两人万万没想到自己会出现在千里之外的斯诺登的镜头里。斯诺登一眼就认出了他们，其中一个来自人力资源部，另一个则是局里的巡查人员。[276]他明白，留给自己隐匿身份的时间不多了。

正在等待自己的第二篇文章发表的格林沃德也再度紧张起来。《卫报》方面正在就这篇报道“棱镜”计划的文章和白宫方面斗智斗勇。有了上一篇文章的“斗争”经验，吉布森这次的表现更加游刃有余。她告诉格林沃德，稿件将于半小时后发表。格林沃德非常高兴。就在这时，他接到吉布森发来的消息，内容完全出乎意料，他几乎不敢相信自己的眼睛：《华盛顿邮报》刚刚发表了关于“棱镜”计划的文章！[276]

这一次，《华盛顿邮报》终于抢在了《卫报》的前面，成为首家报道“棱镜”计划的媒体！

第六回 “棱镜”！“棱镜”！

2009年11月底，《华盛顿邮报》悄悄宣布，由于经费紧张等原因，报社将关闭在纽约、芝加哥和洛杉矶的三个办事处。几年前，报社就关掉了在奥斯汀、丹佛和迈阿密的三个办事处。这次关掉纽约等三个办事处意味着报社设在美国国内的所有外派机构都将不复存在。报社哀叹，困守华盛顿，就只能通过“华盛顿棱镜”（Washington prism）报道美国国内的情况，事件发生当地的人们的某种看法肯定会被过滤掉，对事件的报道必定不能像先前那样全面和及时。这一波裁员波及6名记者，不过报社已经安排他们回华盛顿工作，其余辅助人员则就此被解聘。这6人当中就有戈尔曼。[405]

不过，戈尔曼并没有到华盛顿工作的打算，而是很快在纽约找到了自己的下家：总部位于纽约的《时代》周刊。他和杂志社商量好，将负责打理一个专栏。与此同时，他还进入纽约大学法学院，成为这家学院下面法律和安全中心的高级研究员。[406]在《华盛顿邮报》工作20多年、两度获得普利策奖，其中一次获奖的系列文章曾作为底本，被演绎扩充成一部讲述副总统切尼故事的《垂钓者》，一经出版，好评如潮，被《纽约时报》《华盛顿邮报》《洛杉矶时报》和《哈波斯》杂志等媒体，以及亚马逊和巴诺书店评为2008年度最佳图书。简历上有了这几条，基本上是可以“走遍天下都不怕”的。

连环炮

2013年2月初，波伊特拉斯跟戈尔曼取得联系。他们都曾是纽约大学法律和安全中心的研究员，彼此认识。第一次见面，两个人先按照约定到纽约市西区的一家咖啡店碰头，为了防止被跟踪，他们又走到另一家咖啡店，然后才坐下来谈正事。[279, 407]

波伊特拉斯告诉戈尔曼，一个月前有个神秘线人找到自己，说是有重大线索想要爆料。这个神秘人提醒她，需要用足够长、足够复杂的字符串来做密码口令，“要假设你的对手每秒可以猜测上万亿次”[354]。她还把一些谈话记录拿给戈尔曼看，想请他帮着辨别一下真伪。多年来，戈尔曼投入大量的时间和精力调查美国政府的大规模监视行动，波伊特拉斯的这些材料印证了他已经掌握的情况，并且非常可信地填补了若干他还不知道的空白。戈尔曼几乎立刻就相信了这个神秘线人的真实性。[408, 409]当然，现在已经知道，这个线人就是斯诺登。

接下来，戈尔曼就和斯诺登直接进行联系。他比格林沃德更理性，更有保密方面的经验。斯诺登自称“Verax”，他给戈尔曼起了一个代号，叫“黄铜标牌”。相比于在格林沃德那里碰了“软钉子”的状况，斯诺登与戈尔曼的交流顺畅得多。然而，刚开始的时候，斯诺登还是对主流媒体的记者心存疑虑，他不断试探：戈尔曼愿不愿意接下这个任务，而《华盛顿邮报》愿不愿意支持他。斯诺登当然不是骗子，面对记者提出的种种问题他总能给出合情合理的回答。在戈尔曼眼里，即使没有后续提供的文件，斯诺登也是一个非常可信的爆料人。[408]

但斯诺登带给戈尔曼的显然远远超出了预期。戈尔曼最初只是以为，能够从这个线人那里得到的，也就是一两份文件而已。他清楚地记得，有一天，对方传来一份文件，是有关“棱镜”计划的那套幻灯片，而第二天对方竟传过来多份文件，用戈尔曼自己的话说：多到“自己的下巴都掉了下来”[408]。

说到戈尔曼，在其母校普林斯顿大学里，他还有个绰号，叫“82届的戈尔曼”。当他还只是一个大学生的时候，就做过学校里非常有名的学生报纸《普林斯顿人日报》的主编，从那时开始，他就已经是一名出色

的记者了。他毕业论文的主题是关于1925届校友乔治·凯南（George Kennan）的。这位凯南曾经化名“X”，在《外交事务》杂志上发表文章，明确提出美国应该对苏联进行长期、耐心的“遏制”，并由此获得“遏制政策之父”的称号。戈尔曼这篇论文的成绩是“极优”，他也因此荣获了罗德奖学金，得以到牛津大学攻读硕士学位。[410]1985年，戈尔曼出版了自己的第一本著作《与凯南争辩：通向美国力量的哲学》。后来他作为《华盛顿邮报》的记者，常驻耶路撒冷，近距离报道过“拉宾遇刺”等重大事件。[411]再后来，他前往伊拉克，一口气写出了若干篇重量级文章，告诉大家那里的大规模杀伤性武器核查工作已经失败。[48, 412, 413]

根据自己丰富的工作经验，戈尔曼认为斯诺登提供的材料更适合在《华盛顿邮报》上发表，他需要“整个报社团队的支持”，而这是《时代》杂志社无法做到的。于是他回过头，找《华盛顿邮报》的总编和副总编商量此事。报社对戈尔曼提供的线索非常重视，马上着手开展工作。不过，有点儿不同寻常的是，报社这次并没有把他安排在5层——尽管那里是记者们工作的主要楼层，而是把他放在了7层，那里离报社的法律部门更近。[414]这样的安排，一是可能出于保密方面的考虑，二是可能因为报社已经预料到，即将出炉的爆炸性新闻有许多法律问题需要解决。

从第一次接触斯诺登开始，戈尔曼就有一种强烈的直觉，这个神秘线人的真实性很强，他所说的很可能是真的，但他很好地保持了理智。在相当长的一段时间里，他反复验证斯诺登所说的话，以及他提交的材料是否真实、是否准确。[409, 415]他找到自己认识的其他一些消息来源人士，向他们求证。即便这些人非常可靠，他也几乎不会告诉他们，自己掌握了如此高密级的材料。这是他的一条原则。之所以这样做，主要是为这些线人减少不必要的麻烦，因为一旦他们知道这些情况，按规定必须向有关部门和领导报告。对于自己的这段求证过程，戈尔曼是这样说的：

我找到我非常信任的一些人，我们大概会先聊一些无关痛痒的话题。然后，我说：“假设有个记者跟你说，他知道更多情况，他知道他‘不应该’知道的情况，你是希望那个记者告诉你这些情况，还是对他说‘滚出去’？”这两种回答，我都得到过，在不同的时候、从不同人那里。[408]

戈尔曼非常清楚，将要报道的事情牵涉许多法律问题，更需要谨慎对待。为此，他在文章发表前的每个关键节点都要听取来自律师方面的意见和建议。戈尔曼也非常清楚，尽管已经非常小心，但政府方面对曝光和披露内幕表现出严查之势，越抓越紧，自己还是有可能被传唤。不过他相信，只要坚持在法律允许的范围内做事，最终不会惹上太大的麻烦。[408]

和对待格林沃德一样，斯诺登也向戈尔曼公布了自己的真实身份。他不是简单地说我是某人，而是把自己的姓名、社会保险号、政府工作号以及作为中情局雇员的身份信息都告诉了记者。但斯诺登没有透露自己的出生日期，因为这件小事，戈尔曼心里还有点儿打鼓。不过他并没有立即用斯诺登坦白的那些身份信息查验真伪，而是等到有关“棱镜”计划的那篇文章基本写成后，才着手解决疑惑。看到检索出来的出生年月，戈尔曼怀疑数据有误，因为对方实在太年轻了。[408]系统数据没有错误，这的确是一个很年轻的小伙子！

前面曾经提到，戈尔曼听从了律师的建议，拒绝了斯诺登让他到香港见面的邀请。但是自始至终他对格林沃德等人的行踪都了如指掌，因为他一直和波伊特拉斯保持联系。[408]他知道三个人如约见到了斯诺登，知道格林沃德在没日没夜地疯狂写作，也知道他们除了第一篇已经抢先发表的报道，手里还有一系列文章已经基本准备妥当，特别是他们也有一篇关于“棱镜”计划的报道。

为了发表曝光“棱镜”计划的文章，《华盛顿邮报》照例也需要跟政府“协商”。戈尔曼事后回忆说：

政府最希望我们做的是不要提这9家公司的名字。简单地说，他们的理由就是，如果报社曝光出来，他们将无法继续跟商业公司合作。而我的回答是：“这正是我们要点出他们名字的原因。”我们并不是为了某个特定的结果，也并非想破坏你们跟公司的合作，但如果你们所说的对公司名誉上和商业上的损害，是因为他们或者你们做了公众不喜欢的事情，那么报道这些事情就是我们应尽的责任。[416]

据说就在这个时候，有官员悄悄给《华盛顿邮报》的高层透露了风声，说政府同时还在跟《卫报》协商此事，而《卫报》给政府预留的时间很短。这就意味着，如果不加快进度，率先报道“棱镜”计划的将是《卫报》，而不是《华盛顿邮报》。时不我待，必须当机立断。《华盛

顿邮报》决定，马上发表戈尔曼撰写的文章，文章不仅署了戈尔曼的名字，还署上了波伊特拉斯的名字。这一天是2013年6月6日。在这篇文章里，戈尔曼写道：

《华盛顿邮报》获得的一份绝密文件显示：国家安全局和联调局直接从美国9大互联网公司的中心服务器上截取数据，包括语音和视频聊天、照片、电子邮件、各类文档以及连接日志等，帮助情报分析人员跟踪国外目标。

这一计划代号“棱镜”，在此之前一直不为人所知。这样的计划可能史无前例。国安局擅长窃取秘密、破解密码，它也习惯于借伙伴之力分流数据、规避障碍。但是它还从未有过像谷歌和脸谱这样的伙伴，也从未接触到比硅谷所拥有的更为丰富的高价值情报源。

同样非同寻常的是，国安局抽取他们所需要的数据的方式。这份材料显示：“（国安局）从以下这些美国互联网服务提供商的服务器上直接搜集数据：微软、雅虎、谷歌、脸谱、聊天软件PalTalk、美国在线（AOL）、Skype、优视和苹果。”[417]

需要说明的是，这里转引的是一天后悄悄发布的修订版本。相比于原始版本，戈尔曼又做了不少工作：扩充了近一倍的内容，对多处内容进行了修正、润色和完善，并且稍微修改了文章的标题。原始版本在《华盛顿邮报》官网上已经无处可寻，但还是有人眼疾手快，保存了两个版本并且进行了比对。[418]戈尔曼事后感慨，如果能再多一两天时间准备就好了。[414]总而言之，为了赶时间，《华盛顿邮报》仓促发布了关于“棱镜”计划的报道文章，这篇“急就章”并不能令人满意，但的确在时间上“领先”一步，那么他们的竞争对手《卫报》又在干什么呢？

直到有关威瑞森公司的报道发表之前，白宫仍然不相信《卫报》胆敢如此行动。美国国家安全委员会发言人凯特琳·海顿给《卫报》的代表发了一条短信：“你们这帮家伙真要按计划进行了？”[367]但随后发生的事情让美国政府从此对这份来自英国的报纸另眼相看。

《卫报》如此“不听话”，美国政府当然就不用再客气了。报社的办公楼下突然出现了一群挖路工，三下五除二就把楼前的人行道挖得一片狼藉。主编吉布森家门口也冒出来一群不速之客，开始轰轰隆隆地施工。与此同时，《卫报》华盛顿办事处门外似乎也需要改造，一支施工

队赶来，干得热火朝天。更加诡异的是，报社的办公笔记本电脑开始反复死机。当吉布森跟格林沃德通过网络进行加密聊天时，计算机和网络开始经常崩溃。她半开玩笑半当真地说："很快，我们就要被迫更加擅长情报技术了。"参与"斯诺登事件"报道的这些人原本并不熟悉加密技术，后来都成了加密方面的行家里手。[367]

报社总编拉斯布里奇专程从英国飞到了纽约，亲自督导接下来对"棱镜"计划的报道工作。和上一篇有关威瑞森的文章类似，报社这次也派出专人与有关公司接洽，不过，这些公司都矢口否认自己和国安局串通一气。[367]

除此之外，跟政府沟通的程序也是必须要走的。白宫方面反对发布任何一张涉及"棱镜"计划的幻灯片，《卫报》反复斟酌，从41张幻灯片里挑选了三张发表。这算得上是非常保守的一种做法了。这三张幻灯片中就有一张披露了微软、雅虎和谷歌等公司加入"棱镜"计划的具体日期。负责跟白宫沟通的吉布森说："我们需要发表这一内容。这是我的底线。"她还告诉对方，文章计划发表的时间是当天下午6点。[367]

报道准备工作按计划紧张进行，但是他们的进度被《华盛顿邮报》探听到了，《华盛顿邮报》最终抢先一步发表了文章。吉布森几乎在第一时间得知了此事，她立刻就把这一情况通报了远在香港的格林沃德。事已至此，也无法转圜。《卫报》只能继续按照原定计划行事。十几分钟之后，《卫报》的美国分社网站上登出了他们对"棱镜"计划的报道文章，署名是格林沃德和麦卡斯基尔。[276]文中写道：

《卫报》获得的一份绝密文件显示：美国国家安全局可以直接访问谷歌、脸谱、苹果等美国互联网巨头的系统。

该文件显示：国安局能够这么做源于一个从未被披露的"棱镜"计划。该计划允许（国安局）官员搜集美国公民的搜索历史、电子邮件、上传文件、在线聊天等各种数据。

这是一份PoPowerPoint幻灯片，看来是培训情报人员用的材料。文件的密级标为"绝密"，不允许交给外国盟友。《卫报》验证了文件的真实性。该文件宣称：（国安局）从主要的美国互联网服务提供商的"服务器上直接搜集数据"。[419]

“追溯豁免”

微软公司第一个加入“棱镜”计划，其实一点儿也不意外。“9·11”事件发生后不久，微软公司里就不时出现联调局特工的身影。他们手拿法庭指令，要求公司提供用户的账户和电子邮件信息，并且通常要得很急。公司的工程师把数据整理好之后提供给政府部门。有时候因为没有合适的软件工具，工程师们只能手动整理这些数据。微软公司内部把这项工作叫作“胡佛”。[420]

前面曾经提过，2007年1月，外国情报监视法庭签发了第一份有关互联网内容和电话内容的法庭指令，官方说法是“总统监视计划”从此结束，但实际情况是：原先4项任务通过总统指令获得授权，从这之后改为通过法庭指令获得授权。变化仅此而已，大规模搜集美国国内通信数据的“星风”行动并未停止。即便如此，小布什政府还是颇为不快，威胁说改由法庭指令授权之后，反恐情报出现了“缺口”，催促国会尽快在法律层面提供解决办法。[421]

于是就有了《保护美国法案》。小布什政府设法让国会通过了这部法案，对《外国情报监视法案》做了进一步的修订。原先法庭指令必须明确需要监视的特定目标，有了《保护美国法案》，法庭指令便可以笼统地涵盖一大批监视目标。白宫轻描淡写地把这个法案说成是对《外国情报监视法案》的一次“技术性修订”，是为了弥补原有法案在反恐形势下的不足。[422]简而言之，他们试图掩盖这次修订的深意，但他们的这些说法只能糊弄不太懂法律的普通人。具有哈佛大学法学院专业背景的奥巴马当然清楚这些修订的意义。他当时作为参议员，正在竞选美国总统，对《保护美国法案》投了反对票。在投票之前，他还讲了这么一段话：

本届政府在我们珍爱的自由和保障安全之间做出了一个错误的选择。（如果当选，）我将为情报部门和执法部门提供他们需要的工具，在追踪和消灭恐怖分子的同时，确保美国宪法和我们的自由不被削弱。[420]

但这部《保护美国法案》最终还是以60：28的投票结果在参议院获得通过。众议院也在同一天通过了这部法案。正是这样一部法案，直接

催生了一个新的秘密计划，这就是“棱镜”计划，按照惯例，国安局内部赋予它一个“信号情报行动编号”（SIGAD）——“US-984XN”。就在参众两院通过法案后一个月，微软公司率先加入“棱镜”计划，现在看来，他们选择了一个非常有意义的日子，2007年9月11日，正好是“9·11”事件的6周年纪念日。

有人事后评论说，《保护美国法案》实际上“扫荡”了《外国情报监视法案》。按照这部新法案的规定，有关部门只需要“证实”某项监视行动的“主要目的”是对外情报任务，并且该行动设置了若干“合理的程序”，有足够的把握，监视目标是身处美国之外的人员，就可以启动监视任务。签发的每个指令都可以涵盖非常宽泛的监视人群，而对于某个已经被认可的行动计划而言，也不再需要对单个监视目标进行合法性审查。[422]

美国的民权组织看到这样一部法案出炉，大吃一惊。他们曾经猜测，政府可以宣称为了全面获得恐怖嫌疑人的各种信息，不受任何限制地拿到国内通信数据。他们的这种担心最终成为现实。[422]

《保护美国法案》“修正”了《外国情报监视法案》的若干重要内容，好在这只是一部有效期仅6个月的临时性法律，影响并不算长久和深远。相比之下，2008年大选期间的热门话题、《外国情报监视法案》（修正案）对美国社会带来的影响则深刻得多，甚至可以说是恶劣得多。前文讲述前美国国家情报总监麦康奈尔的时候，曾经提到“追溯豁免”这个概念，这是指通信公司参加政府认可的监视行动，不论行动发生在过去、现在还是将来，也不论这一行动是否合法，通信公司都将获得豁免、不被追责。这样一种“追溯豁免”原本是《保护美国法案》的一条内容，因为众人反对，在法案通过时被国会删掉了。但是，到了2008年，一番激烈的争论之后，能言善辩的麦康奈尔等人成功说服国会通过了《外国情报监视法案》（修正案），把“追溯豁免”加进了这部法案，有效期4年。简单地说，这部《修正案》固化和强化了《保护美国法案》的内容，2012年几乎一字未改，在国会再次获得通过，有效期一直到2017年。[17, 422]

就在这部修正案通过前后，雅虎公司以及自称“不作恶”的谷歌公司签字加入“棱镜”计划，然后是脸谱、PalTalk、优视等公司，最后一个是2012年加入的苹果公司。这些公司为“棱镜”计划做的所有事情在法律方面的依据就是《修正案》第702条，这条法案的核心内容其实只有一句

话，只要拿到司法部部长和国家情报总监两个人的签字，只要有关部门“有理由”相信某个人身在美国之外，这些部门就可以对他进行监视、获取情报，有效期最长一年。监视对象则是除美国人以外的所有人。这一条法案要求，不允许故意监视美国人，即使他身在美国之外。

在2008年参议院投票通过《外国情报监视法案》（修正案）的时候，只有怀登和菲因高德投了反对票，最让他们不安的就是这个第702条。菲因高德说：

我是参议院里有权听取无证监视计划完整汇报的少数几个成员之一。我可以保证，如果有朝一日解密了这个计划的更多信息，这是很有可能发生的……（到那时，）各位议员都会后悔，我们怎么会通过这样一部法案。[423]

有了“追溯豁免”，参加监视行动的公司便无须考虑法律方面的问题。这也必然有助于政府拉更多公司入伙、参加秘密计划。斯诺登曝光的“棱镜”计划材料清楚地显示，美国政府除了与微软等9家公司签约，还有许多合作伙伴。不过这些伙伴姓甚名谁，到目前为止，仍然是一个巨大的秘密。法律方面的问题虽然避免了，但经济方面的风险必须承担。2014年6月，威瑞森下属的德国分公司突然接到通知，他们和德国政府部门签订的合同将在一年后终止。在此之前，这家公司为许多德国政府单位提供互联网服务。对此，德国内务部发言人是这样解释的：有证据显示，威瑞森需要向美国国安局提供信息，德国政府与该公司的合作关系只能中止。[424]德国分公司很是委屈，发表声明说“威瑞森（德国）公司是一家德国公司，恪守德国法律”[425]。可惜，他们的说辞无法改变德国政府的决心。德国人对默克尔总理被长期监听一事非常恼火，一段时间以来一直琢磨着如何反击，中止威瑞森的合同只是他们给了美国人一点儿“颜色”而已，公司方面因此遭受损失也只能怪自己运气不太好吧。

要么加入，要么消亡

《卫报》登出有关威瑞森公司的报道时，很多人认为这可能只是一次“孤立的”曝光事件，没想到第二天《华盛顿邮报》和《卫报》竟然几乎同时抛出了揭露“棱镜”计划的重量级文章。看了戈尔曼和格林沃德等人撰写的文章，大多数人取得了这样一种共识：美国国安局在私营公司的配合下，直接侵犯了美国人的通信自由和通信隐私。

当然也有其他一些声音冒了出来。他们说，“棱镜”并非获取通信数据的计划，而只是一种计算机系统。有好事者搜索到硅谷的一家公司，他们开发的数据集成软件也叫“棱镜”。这家名为“帕兰特”的小公司的行迹看上去十分可疑，因为他们的实际投资者之一是中情局。面对这样的猜疑，帕兰特公司立刻发声，撇清关系，并且说他们研发的系统主要应用于银行而不是政府部门。[426]

还有人找出帕兰特公司若干年前发布的一份报告，其中提到美军太平洋司令部已经在使用的一个情报搜集管理软件，全称是“资源集成、同步和管理计划工具”，首字母缩写碰巧也是“棱镜”，由于这个系统被用于情报监视和侦察工作，猛地一看，还真像那么回事儿。[427]

美国国家情报总监克莱伯有点儿坐不住了，先后发表了若干份声明，其中一份写道：“棱镜”是政府内部使用的一个计算机系统，用于提高政府有关部门依据法令并在法庭的监管下，从电子通信服务商那里获取数据的效率。该说法的前半句很大程度上是希望利用“系统”这个概念的模糊性，让普通人觉得“棱镜”只是一个很小的东西，最好能马上忘记，而后半句还是比较真实的。一时间，“‘棱镜’是什么”这个简单的问题硬是被有意无意地搅成了一摊浑水。克莱伯还说：

（“棱镜”计划的）所有信息搜集工作都是在司法部部长和国家情报总监书面授权之下进行的，并且经过了外国情报监视法庭的批准，服务商也都知情。[428]

戈尔曼最初撰写曝光“棱镜”计划的那篇文章时曾经提过，那几家公司是在事先知情的情况下参与这个秘密计划的，跟克莱伯总监的说法一致。可惜，被曝光的几家公司似乎并不认同总监的这一说法。尽管有“追

溯豁免”保护，他们仍异口同声地表示“从未听说过”“棱镜”计划。

脸谱公司的创始人及首席执行官马克·扎克伯格（Mark Zuckerberg）说，直到前一天看到新闻报道，自己才得知此事，他没有听说过“棱镜”计划，公司也从未参与过任何计划，未允许政府直接访问公司的服务器。谷歌公司的联合创始人佩奇也发表声明，否认事前知道“棱镜”计划，也否认谷歌允许政府直接访问公司服务器，不过他倒是承认曾合法地向政府提供数据，宣称“公司的法律部门对每次数据提供的每个要求都进行审查，并且经常拒绝过于宽泛的要求和不按程序提出的要求”。[429]

迫于压力，戈尔曼后来在修改文章的时候悄悄去掉了“事先知情”的有关词句。不过，这些公司的说法并不能让人信服。理由很简单：在公司内部开展这种大规模的数据搜集行动，公司方面不可能一无所知，更何况国安局每年还要付给这几家公司2000万美元作为“辛苦费”。[430]虽然这笔钱在平分给各公司之后相对于它们的营业收入而言实在微不足道，但毕竟也是真金白银吧。也许真的是数量太少，公司上层不放在眼里就抛诸脑后了。

有人看到这几家“涉案”公司全都在否认，就猜想，政府部门“直接”获取数据是通过在这些公司的电缆上直接搭线实现的，因而公司可能确实毫不知情。[431]为了进一步澄清事实，《卫报》在6月8日刊登了一张新的幻灯片，不过对片子做了两处涂黑处理。[431]7月10日，《华盛顿邮报》“重新”公布了这张幻灯片，他们发布的这个版本未做处理，人们终于能够一睹其全貌。

有人说“棱镜掌握一切”，这其实是一种非常错误的说法，利用大多数人只听说过“棱镜”这个名词，误导大家形成错误的概念，认为“棱镜”就是美国国安局监视计划的全部。这张幻灯片上清楚地写着，对于情报分析人员，应该使用两类数据，一类是通过上游的若干个计划得到的数据，另一类是“棱镜”计划搜集到的数据。这两类计划在法律方面的依据都是《外国情报监视法案》（修正案）的第702条，也因此统称为“702”行动计划。这也说明，“棱镜”计划只是国安局诸多监视计划中的一个，说它“掌握一切”，与实际情况相差了十万八千里。

这张幻灯片上最引人注目的一句话是，借助于“棱镜”计划，国安局可以“直接从美国的互联网服务提供商的服务器上搜集数据”。这句话也

正是《华盛顿邮报》和《卫报》的报道依据，但显然和几大公司的说法完全不同，也就自然而然成为个别人抨击这些报道的“把柄”。究竟真实情况如何，谁是谁非现在还不知道。但至少可以肯定，从公司服务器上获取数据是的的确确在发生的事情。

退一步说，其实“直接”还是“不直接”并不像公司强调得那么重要。只要增加一点儿技术手段，比如在公司的一些重要地点部署属于美国政府的服务器或者服务程序，利用这些硬件或者软件作为桥梁，完全可以实现“间接”从公司的服务器上抓取数据。这并非胡乱猜测。据《纽约时报》披露，至少在与谷歌和脸谱公司的谈判中，政府部门就曾提出，要在公司服务器上建立独立的安全门户，由政府部门提出数据请求，公司根据请求把有关的数据筛选出来再存进去，然后有关部门再通过门户把数据调出来。[432]简而言之，关于“直接”还是“不直接”访问公司服务器这个问题，公司方面很可能只是在玩文字游戏。

《华盛顿邮报》从美国情报界的消息源处获知：尽管从技术上讲“直接”从公司的服务器上获取数据这句话不够准确，但基本符合情报分析人员的感受。分散在世界各地的国安局员工如果得到了访问“棱镜”计划数据的授权，他可以在自己的计算机上设定监视任务以及获取数据的条件，然后就等着从互联网公司那里拿到监视数据。[428]这样的过程也可以算是“直接”吧。

但有时候，即便能够拿到公司服务器上的数据，使用起来也不容易。2012年7月，微软公司刚开始测试一种新的服务产品Outlook.com，国安局就发现要解读这个网站上加密的聊天信息不太容易。于是由联调局出面协调，微软公司提出一种方法，让国安局绕过这个网站的加密机制读取聊天信息。几个月后，国安局发布内部文件宣称，公司提供的方法已经“在12月12日通过测试并投入使用”。2013年2月，Outlook.com正式上线。善良的用户们并不知道，从第一天起，这个网站上的所有聊天信息不管是否加密，国安局都可以很容易地拿到。不仅是聊天信息，甚至连微软公司旗下所有的电子邮件服务产品，包括Hotmail、Live和Outlook，国安局都能够拿到加密前的数据。除此之外，公司主打的云存储服务品牌SkyDrive也对国安局敞开了大门。[433]

当然，政府部门与公司的合作并非总能如此顺畅。2007年下半年，为了开展监视活动，美国政府找到雅虎公司，没想到竟碰了一鼻子灰。

雅虎公司辩称，政府方面要求公司在没有调查令的情况下提供用户数据，如此无限制的命令侵犯了《宪法第四修正案》赋予公司用户的权利，属于无理的搜查和攫取。外国情报监视法庭则认为，公司的这一担忧“言过其实”，并且说，尽管公司方面“描述了诸多骇人听闻的情形，但并没有提供证据证明这样做会造成何种伤害、有何种异乎寻常的过失风险，或者有任何宽泛的滥用可能性”。摆在雅虎公司面前的只有两个选择：要么交出数据，要么面临惩罚。最终，雅虎公司不得不屈服，加入“棱镜”计划的队伍之中。[434]根据后来曝光的法律文件，这一天是2008年5月12日[435]，这一点和幻灯片上的日期不一致，估计有可能是幻灯片作者的一个小小的笔误。

“棱镜”计划曝光后，雅虎公司向外国情报监视法庭递交了一份公开文件，要求解密2008年案件的有关材料，因为从这些材料可以看出，公司曾经极力反对那些强加给他们的法庭指令，但他们的各种反对意见都被法庭驳回了，甚至他们提出缓期执行这些指令的请求也遭到拒绝。[436]经过一年的努力，2014年9月11日，雅虎公司得到允许，公开了1500页诉讼文件。到此时，人们才看到，当时的国家情报总监麦康奈尔曾经专门签发过一个声明，他在其中“声色俱厉”地写道：

雅虎公司拖延执行法庭指令，每一刻都有可能对美国的安全带来巨大的危害。他们不遵照法庭指令（提交数据），每一天都会给外国情报信息带来无法弥补的损失。[435]

事后看来，总监的这番话还真有点儿“即使是响鼓，也需要重锤敲”的意味。据国安局统计，“棱镜”计划中大约98%的成果出自雅虎、微软和谷歌三家公司提交的数据。[417]而据国安局内部的统计，三家公司中，雅虎公司的“贡献”最为突出。斯诺登提供了一张幻灯片，上面很直观地显示出，在一段时间里，相较于其他公司，雅虎公司相提供的数据是最多的。从这也就能够理解，国安局为什么紧盯着雅虎公司不放：如此重要的公司是无论如何也不能让它游离于“棱镜”计划之外的。

在斯诺登提供的幻灯片里，有一张专门介绍“棱镜”计划的情报编号方法。编号分为5段。第1段是情报来源，从“P1”到“P8”以及“PA”，一共9个，分别对应参加“棱镜”计划的公司。幻灯片上举了一个例子，第一段的内容是“P2”，说明这份情报来自雅虎公司。第2段从字母“A”一直排到字母“J”，分别代表10种情报内容类型，如果情报比较复杂，包含了多种类型的内容，就用一个“.”表示。在幻灯片上，如果第2段的内容是

字母“E”，表示这份情报是雅虎公司的一份电子邮件。对于第3段，所有通过“棱镜”计划搜集到的情报都有“SQC”三个字母。第4段是年份，第5段是流水号。正是因为雅虎公司对“棱镜”计划做出的贡献极大，给国安局员工留下的印象深刻，所以信手拈来的典型示例才非它莫属。

除了情报总监的训斥之辞，雅虎公司还获准公布一份法庭文件，其中直截了当地威胁道：如果公司拒绝提交数据，他们将面临每天25万美元的罚款，并且每拖延一周，罚款还将翻倍。[435]看到这里，世人终于了解到：当年美国政府施加在雅虎公司身上的压力有多大，不仅有政治上的，还有经济上的，“两手都在抓，两手都很硬”。这次能够披露若干年前的秘密诉讼文件，终于让雅虎公司压在心底的怨气稍稍得到了一点儿宣泄。

在9家参与“棱镜”计划的公司中，优视公司在加入计划之前就已经被谷歌公司收购，而Skype公司则是在顺利加入计划之后8个月，被微软公司收购的，所以实际上应该是7家公司。据了解内情的人士称，为了给政府情报部门和执法部门使用Skype通话数据提供便利，Skype在内部还启动了一个秘密的配套计划，叫作“国际象棋”。即便如此，Skype在公开场合的宣传口号仍是：用户的通话是不可能被窃听的。等到“棱镜”计划曝光，媒体找到微软公司，他们完全不承认曾经有过这样的说法。[437]其实此时此刻，微软公司自己也遇到了类似的麻烦。就在2013年4月，公司发起了新一轮的市场营销活动，他们的口号是“您的隐私问题，我们的当务之急”。[433]在这样的宣传下是如此残酷的现实，实在不知道微软公司将如何自圆其说。

有人发现，名气不太大的PalTalk加入了“棱镜”计划，相比之下名气大得多的推特公司反而缺席了。[417]从推特公司的历史来看，他们对政府的种种命令从来不是简单地顺从，但也不知道他们运用了什么“秘籍”成功逃脱了“棱镜”计划，但这至少可以说明，逃脱还是有可能做到的。当然，这并不意味着推特公司从来不向政府部门提供用户数据，不加入“棱镜”计划只是表明，他们没有专门提供给政府部门一种获取大量数据的捷径，情报分析人员不能简单地登录某个门户，发送数据请求然后就等着数据传到手上。[438]对于“缺席”“棱镜”计划，推特公司的发言人是这样说的：

我们已经表述过多次，推特的用户是推文的所有者。面对政府不合法的请求，用户有权利抗争。在这样的抗争中，我们和他们站在一起。

[439]

除了推特，还有几个名字值得一提。

还记得前文提到的斯诺登用过的那个名为“辛辛纳图斯”的邮箱吗？没错，是“cincinnatus@lavabit.com”。这个邮箱的提供者Lavabit是一家小型的加密邮件服务商，用户只有41万。“斯诺登事件”爆发后，美国政府要求Lavabit公司交出用户密码，他们以为拿到密码就可以快速破解用户的加密邮件。但据说公司掌握的用户密码都经过了“安全哈希算法”的处理，也就是说，即使拿到了这些密码数据，要得到用户密码也不容易，更别说破解用户的加密邮件了。[440]更出乎政府部门的预料的是，Lavabit公司拒绝提供用户密码数据。接下来发生的也超乎公司创始人和运营人拉达尔·列维森（Ladar Levison）的预料，他很快就收到了法院的传票，由于案件特殊，原先公司聘用的律师根本进不了法庭，公司失去了所有法律方面的援助。最终，列维森输掉了官司，他的面前只剩下三条路：交出用户数据，或者成为危害美国人民的犯罪同谋，或者关掉这家公司。2013年8月，他发表了一封公开信，放弃了这份自己辛苦经营了10年的事业。[441]在信中，他发出了这样的警告：

我强烈建议，任何人都不要相信与美国有实际联系的公司，不要把自己的私密数据交给他们。[441]

就在列维森宣布关闭Lavabit公司几个小时之后，另外一家小型电子邮件服务商Silent Circle也宣布终止自己的加密邮件服务，他们认为与其在收到法院传票或者法庭指令之后被迫关闭这项服务，不如自己动手主动砍掉这块业务。[442]

“上游”四计划

所谓“上游”，并不是指某个具体的计划，而是四个秘密计划的统称，它们的代号分别是“布拉尼镇”（BLARNEY）、“锦绣镇”（FAIRVIEW）、“风暴酿”（STORMBREW）和“橡木星”（OAKSTAR）。相对于这四个秘密计划，“棱镜”就是一个“下游”计划。[443]“风暴酿”和“橡木星”这两个代号在《卫报》第一次发布“棱镜”幻灯片的时候曾被涂黑过。这四个代号后来在斯诺登提供的若干张幻灯片上出现过。

据《华尔街日报》披露，国安局官员私下开玩笑说，把秘密监视计划叫作“布拉尼镇”，意在向许多年前的“三叶草”行动计划致敬。[444]把“布拉尼镇”和“三叶草”关联起来的，有一个关键词——“爱尔兰”。

在爱尔兰人的世界里，三叶草具有特殊意义，它那三片心形的叶子连在一起，看起来最能体现宗教上的“三位一体”，三叶草不仅被爱尔兰人选作国花，还成为他们的传统节日“圣帕特里克节”的象征。

“布拉尼”的原意是“花言巧语”，它既是爱尔兰一个小镇的名字，也是这个小镇上一座古堡的名字，更具体地说，是城堡里的一块著名石头的名字。这块石头的名气源于一个神乎其神的传说。据当地人说，亲吻这块石头可以让人变得能言善辩。不过，想做到这一点并不容易，需要仰躺着、用手抓住护栏，把身体弯成一张弓的样子。即便如此困难，还是有很多游客甘愿一试。在国安局的幻灯片上，三叶草的旁边还有一顶绿色的帽子，它同样属于爱尔兰，是传说中的一个魔法精灵，个子矮小，却藏有一罐宝藏。

为了更好地保密，国安局总是使用代号来代指某个项目、某个行动或者某项计划，甚至参与行动和计划的公司、企业甚至个人都有掩护的代号。对国安局历史颇有研究的艾德发现，大多数代号看不出什么实际意义，就像是随机挑出来的某个单词而已。这样做显然有一个好处：局外人很难根据代号猜出这些行动或者计划的性质和内容，也很难猜出到底是哪些公司、哪些人参与其中。[445]不过，“布拉尼镇”这个代号多半是用心挑选的，只是不知道国安局为什么有这么深的爱尔兰情节。

前面曾经提过的“创始人”、“开拓者”以及“棱镜”，隐喻的意味十足，估计这几个代号多半也是精挑细选的。艾德认为，“锦绣镇”的背后是美国电话电报公司，“风暴酿”的背后是威瑞森公司。[445]《华尔街日报》则认为“布拉尼镇”的背后是美国电话电报公司。[444]总而言之，这几个代号掩护的是哪些公司至今说法不一，仍然是个秘密。

与“棱镜”计划不同的是，处于“上游”的这四个秘密计划有一个共同特点，它们都是直接从光纤电缆上抽取互联网通信数据，而和“棱镜”计划相同的是，国安局照例也要向这些商业伙伴支付一些“辛苦费”。在2013财年，“布拉尼镇”、“锦绣镇”和“风暴酿”的预算依次为6596万、9474万和4604万美元，最少的是“橡木星”，只有941万美元。[446]

在“棱镜”计划的幻灯片里，有一张在标题上写着“美国是世界通信的主干”，其中写道：

大多数世界通信数据流经美国；

情报目标的电话、电子邮件和在线聊天数据，采用的是最廉价的流转路径，而不是物理上最直接的流转路径——这条路径并不总能预测出来；

情报目标的通信数据很可能会流进、流出美国。

麦康奈尔担任国家情报总监的时候，在自己的办公桌前支起了一张巨大的全球互联网流量图，流量大小指明那个国家的大小。在这张图上，美国比其他国家和地区都大。美国是全球最大的网络交换中心，可以接触到海量的元数据，包括电话记录、网络活动和银行交易，情报分析人员可以从中发现异常情况、阻止尚未发生的攻击计划。麦康奈尔曾对一个来访者说，对美国而言，巨大的互联网流量意味着巨大的情报优势。[218]

互联网最初起源于美国国防部的阿帕网（ARPANet）。准确地说，阿帕网从来不是一个纯军用的网络，这在它一分为二的时候变成一个优点：军用部分单独发展，民用部分走向社会、招商引资，少数几家公司成为一级（Tier-1）互联网服务提供商（ISP），也就是人们常说的互联网主干。所以从一开始，互联网的主干就在美国，现在依然如此。在互联网产业中，服务提供商总是处于内容提供商（ICP）的上游，而一级服务提供商可以说是上游中的上游。威瑞森公司、美国电话电报公司、

世纪电信公司以及第三层通信公司（Level 3）就是这样的服务提供商，其总数不超过20家。

需要说明的是，在美国本土这些一级服务提供商的主干光缆上跑的数据，既有来自美国或者去往美国的数据，也有去往世界其他地方的数据。由于互联网基础协议方面的原因，这些数据在到达目的地之前不得不途经美国，这样的数据被称为“过境”数据。这也是“棱镜”计划幻灯片里所说的，“最廉价的流转路径，而不是物理上最直接的流转路径”的确切含义。两个地区之间的数据带宽越大越便宜，就越有可能成为数据流转的通道。

关于不同地区之间的数据带宽，斯诺登提供了一张幻灯片，上面显示得非常清楚：美国与欧洲之间的数据带宽最大，达到每秒4972吉比特，排在第二位的是拉美和加勒比地区，是每秒2946吉比特，亚洲屈居第三，也达到每秒2721吉比特。非洲最少，每秒只有11吉比特。

尽管还不清楚“上游”的四个计划背后是哪几家一级服务提供商，但几乎可以肯定的是，这些计划主要是国安局与美国本土通信公司之间的合作项目。这四个计划的搜集范围并非美国本土的整个互联网流量，而只是其中的过境数据，也就是说，只针对那些出发地和目的地并非美国的通信数据。在前文曾经提过，早在若干年前，国安局就依据第12333号总统令获得了对过境电话通信的跟踪监视权，现在，他们依据《外国情报监视法案》（修正案）的第702条，可以对过境的互联网数据进行跟踪监视。以“布拉尼镇”计划为例，它先后获得了三种授权，最初是《外国情报监视法案》，然后是第12333号总统令，最后是《修正案》的第702条款。每种授权的搜集范围、搜集流程都有所不同。相对而言，要求最“严格”、过程最烦琐的是《修正案》第702条授权，后面还会细述。

对过境数据进行监视，最直接也最有效的方法是跟主干服务提供商合作，在他们的通信线路上搭线监听。在电缆或者光缆上搭线监听的做法历史悠久。1975年，国安局派出一艘名为“大比目鱼”的潜艇，在苏联铺设的鄂霍次克海海底电缆上安装了窃听装置，成功进行了搭线监听。[447]根据国安局内部的一张幻灯片介绍，1978年，也就是“大比目鱼”潜艇出海三年之后，“布拉尼镇”计划就开始了。

除了直接进出美国的数据带宽，值得关注的还有进出欧洲的数据带

宽。欧洲与非洲之间的数据带宽达到每秒343吉比特，与亚洲之间的数据带宽也有每秒1345吉比特。如果能在欧洲以及亚太地区找到合作伙伴，那么来自四面八方的互联网数据就唾手可得。这一点国安局早就想到了。

他们和美国本土以外的网络主干服务提供商展开了广泛的合作。对于英国、加拿大、澳大利亚和新西兰，国安局的合作计划叫作“防风布”（WINDSTOP），其中最密切的合作伙伴当然是英国。关于这个伙伴，先卖个关子，留到下文专门讲。而对于“第三方”国家，国安局的合作计划叫作“护城墙A”（RAMPART-A）。[448]

根据斯诺登提供的材料，所谓的“第三方”国家一共有33个，包括德国、意大利、丹麦、挪威等欧洲国家，以及韩国和日本等亚洲国家。并没有证据证明所有的“第三方”国家都参与了“护城墙A”计划，但比较肯定的是，在这个计划中，德国和丹麦都是国安局的合作伙伴。[448]2011～2013年，国安局用于“防风布”和“护城墙A”这两个计划的经费逐年递减，从9100万美元一路降到5700万美元，不过，两个计划的经费比例基本维持在1：4不变。

德国在这个计划里扮演的角色比较悲剧：一方面，他们与国安局合作开展过境数据监听，是美国的盟友；另一方面，在他们的身后，丹麦也在与国安局合作，而这个国家和德国之间的数据带宽最大，是获得德国过境数据，也就是监视德国的最佳窗口之一。[448]不过，德国也不必为此悲伤，按照国安局内部文件的说法：“我们能够，也经常把第三方伙伴的信号数据作为（监视）目标。”[449]换句话说，美国对盟友的态度差不多都是这样。这也印证了小布什执政时期的美国国土安全部助理部长贝克尔讲的那句话，没错，“盟友未必是朋友”。各位对他这句很刺耳的话应该还有印象。

“附带搜集”

接着说“上游”计划。由于数据过境流量巨大，国安局并不是截获所有数据，而是围绕一定数量的目标“人”搜集情报、进行监视。之所以给“人”字打上了引号，是因为在《外国情报监视法案》（修正案）的字典里，目标“人”既可以是通常意义上的“个人”，也可以是一个“团体”“实体”或者“公司企业”，甚至可能是一股“国外势力”。感觉有点儿晕吧？不晕就不正常了，因为就连戈尔曼这样的资深记者一不留神都会搞错，[450]但法案的的确确是这样规定的，也许是故意的，因为目标“人”的背后有可能是成千上万的真实的人，把他们“浓缩”成一个“人”，普通人就不会意识到监视对象有那么多、涉及面有那么广。

《外国情报监视法案》（修正案）的第702条规定，“锁定”某个外国“人”，需要通过一个“设定”筛选点的过程。筛选点只能是目标“人”的电子邮件地址、电话号码这样的信息，不能是这个“人”的名字，也就是说，“奥萨马·本·拉登”或者“俄罗斯天然气公司”这样的信息不能成为筛选点。并且筛选点还不能是某个关键词，例如“炸弹”或“袭击”。显然，对某个目标“人”而言，可能有多个筛选点。据统计，2013年被“棱镜”计划和“上游”计划，也就是“702”行动计划锁定的各类目标“人”一共有89138个。[451]一旦设定了某个目标“人”的筛选点，他或者他们的有关信息就会被发送给国安局的合作伙伴，针对这个目标“人”的情报搜集过程正式开始。

国安局下属的许多部门都通过“702”行动计划获得情报数据。根据斯诺登提供的幻灯片，截至2013年1月底，筛选点数量最多的是竟然是特搜部。他们设定了29476个筛选点；位列第二的是信号情报分局的中东及非洲产品线，有18061个筛选点；然后是反恐产品线——14945个。尽管筛选点和目标“人”并非一一对应，某个目标“人”可能有多个筛选点，但是从筛选点的数量来看，还是大致可以反映出目标“人”的数量。

上面这些数据反映的是国安局各个部门使用“棱镜”计划和“上游”计划的整体情况。如果单独看“棱镜”计划，设定筛选点的前三名分别是反恐产品线、中东及非洲产品线和防扩散与军备控制产品线；单独看“上

游”四计划，筛选点的前三甲分别是特搜部、中东及非洲产品线和中韩产品线。

这里需要稍微解释一下“产品线”。在美国国安局内部，情报搜集、分析、产品和发布等具体业务由信号情报分局负责，除了分局机关和客户关系部之外，业务部门主要有两个，一个是分析产品部，另一个是数据搜集部。在分析产品部之下，按照地区或者专题，建立了若干个“产品线”。除了上面提到的那4个产品线，还有南亚产品线、俄罗斯产品线，以及国际犯罪与毒品产品线等。

前面曾经提过，“星风”行动的情报分析和报告任务由分析产品部完成，数据搜集任务则由数据搜集部完成。“702”行动计划实际上进行的就是情报搜集和监视工作，都是由分析产品部提出搜集需求，数据搜集部根据这些需求，从合作伙伴那里搜集数据，然后提供给分析产品部。

当国安局看到“棱镜”被广泛关注，而“上游”的四个计划几乎没有引起太大反响时，他们很可能在没人的地方偷偷微笑。因为他们心里清楚，“上游”四个计划的搜集范围比“棱镜”计划广泛得多，既包括互联网数据，也包括电话通信数据，而“棱镜”计划只搜集互联网数据，并且“上游”的四个计划还要多做两件“棱镜”计划不用去做的事情。

第一件事情是所谓的“相关”通信数据搜集。这项工作仅限于互联网通信数据。简单地说，就是国安局的监听对象并不一定参与通信，他可能既不是通信的发起者，也不是通信的接收者，只是他的某些筛选点信息在通信中被人提及，那么这次通信的数据就会被搜集起来以便进一步分析和使用。有点儿不明白？那就举个例子说明一下吧。假如有个美国人，收到某个外国人发来的一封邮件，询问他斯诺登曾用过的“辛辛纳图斯”邮箱具体是什么，美国人就在邮件里说出了答案。国安局显然把斯诺登作为一个重要监听对象，如果他的这个邮箱是国安局的筛选点，那么这封美国人提到斯诺登“辛辛纳图斯”邮箱的邮件就很可能被国安局截获，而如果他又正好使用了某个与美国有着“实际联系”的邮件服务系统，邮件被截获的可能性更大。

“上游”计划做的另外一件事情被称为“多次通信事务”数据搜集。这还真的是一个比较拗口和令人费解的概念。面对《纽约时报》记者查利·萨维奇（Charlie Savage），国家情报总监办公室的官员举了这样一个例子：假如某人有一个基于Web网页的邮箱，每次打开这个邮箱，他都

会看到最新的15封邮件的概要信息，比如说标题、发送日期、邮件大小等。不停地往后翻页，他就能不停地看到更早的邮件，每页都是15封（除了最后一页）。要实现这一点，需要服务程序在后台把15封邮件（也就是15次通信）打成一个包，一次性发送过来，这就是包含多次通信内容的一项“事务”。对“上游”计划而言，如果概要信息中提到了筛选点，那么这15封邮件的概要信息都会被截获。[452]这只是“多次通信事务”的一种情况。

如果监视目标进入某个在线聊天室，聊天室里的其他人都将无辜受牵连，即便是那些只“潜水”、看帖不发言的人，也逃脱不了。按照要求，聊天室里的所有人、他们发的每个帖子、说的每句话都有可能被搜集起来。他们并不知道，不知坐在什么地方的哪个情报分析人员一边写下“一个监视目标、38个无关人员”这样的字句，一边把这些人的数据都搜集起来。[450]

美国政府自己也承认，由于这四个计划包含了“相关”通信数据搜集和“多次通信事务”数据搜集这两个特殊任务，国安局在“上游”计划中比在“棱镜”计划更有可能搜集到纯粹的国内通信数据。[453]为此，有关部门精心挑选了“附带搜集”这个术语来代指这种情况。“附带”这个单词不仅想说明其不可避免，也试图说明政府是无意为之的。也就是说，那些被“附带”搜集的人只能怪自己运气不佳了。

很多人都想知道，到底有多少美国人的通信数据被“附带”了。对于这个问题，国安局局长亚历山大的回答干脆利落：这个数量无法统计。相比之下，国安局总监察官的回答似乎更冠冕堂皇一些，他说：“对这个数量进行估计，会侵犯国安局数据库里存储的美国人的隐私。”[417]不过，在另外一个场合，局长倒是承认，奥巴马总统刚上任的时候，曾经对国安局“附带搜集”的数量之多感到震惊，整个2009年国安局都在处理这些问题。[454]所以，被“附带搜集”的通信数据到底有多少，局长多半是哑巴吃汤圆——心中有数。

为了让新入行的情报分析人员放心行事，国安局在培训时告诉他们，尽管每个季度要汇报一下“附带搜集”的情况，但“没什么需要担心的”。[417]

不难想象，“上游”计划搜集的针对性不如“棱镜”计划强。情报分析人员很可能不得不从一大堆数据里把“有用”的挑出来，使用起来也就不

如“棱镜”计划那么直接和便捷。估计国安局情报分析人员使用“上游”计划的积极性并不高，有数据为证：2011年，国安局的“702”行动计划一共搜集了2.5亿次的互联网通信数据，其中约90%来自“棱镜”计划。如果情报分析人员都不用“上游”计划的数据，那么国安局也就没有必要费这么大的力气实施这四个计划了。

在“上游”计划里，国安局直接与全球志同道合的商业合作伙伴联系，不像在“棱镜”计划中，国安局藏在幕后，由联调局出面，跟美国境内的各大互联网公司打交道。法律规定，“上游”计划搜集到的原始数据只有国安局才有权使用，中情局和联调局只能使用经过国安局处理的二手数据。也就是说，这些数据是国安局相比于其他情报单位的独特优势，所以在“棱镜”计划的幻灯片的内容里，国家权力在“苦口婆心”地敦促情报分析人员：不仅要用“棱镜”计划的数据，还应该使用“上游”计划获得的数据。

作为参议院情报委员会成员，怀登参议员很早以前就知道存在这么一个“棱镜”计划。每次质询情报官员之前，他和助手总要花费很长时间精心准备问题，试图让这些官员的回答最大可能地贴近真相，当然，这个真相涉及秘密、不能点破，最后那层窗户纸只能留给公众和媒体，让他们去猜、去捅了。[423]在2013年3月的一次参议院公开听证会上，怀登参议员抓住机会，当面质问国家情报总监克莱伯。

怀登：国安局有没有搜集成百上千万美国人涉及的任何一种数据？

克莱伯：没有，先生。

怀登：没有吗？

克莱伯：我们没有故意搜集。在个别情况下我们可能无意中搜集到一些，但我们没有故意。[423]

在整个对话过程中，怀登气势逼人，而克莱伯要么眼睛看着桌下，要么躲闪着怀登的目光，他心虚慌乱无法掩饰。[423]在《卫报》有关威瑞森公司的报道发表之后，这段往事被搬了出来，许多人都批评克莱伯，说他撒谎。[455]在怀登提问的那一刻，国家情报总监可能并没有想起“电话通信”“法庭指令”这些事情，在他的脑海中首先蹦出来的很可能是“附带搜集”这样的字眼。“棱镜”计划以及“上游”的四个计划在重要性方面已经明显超出电话元数据搜集计划。国家情报总监后来评价说，

通过“棱镜”计划得到的数据是美国情报界搜集到的“最有价值也最为重要的对外情报信息”。[456]原因很简单，这些数据已经成为美国情报界高端情报产品的主要情报源。

《总统每日简报》

凌晨4点刚过，弗吉尼亚州多半还笼罩在一片黑暗之中，美国国家情报总监麦康奈尔就已经起床了。做了20分钟背部运动之后，他就开始紧张地为每天的必修课——总统情报通气会——做准备了。前一天晚上，麦康奈尔总会收到最新一期《总统每日简报》，上面汇总了各种来源的情报信息，文字简练，条理清楚。清晨6点，一辆黑色的轿车准时出现在他家门外，目的地就是白宫。在车上，他还要阅读一大堆材料，做更加充分的准备，因为谁也不知道在情报通气会上小布什会提出什么样的问题。会议将在7点半到8点之间开始，时间很少超过一个小时，所以他必须尽量把过去一天发生的重要情况都弄清楚，以便在这段不长的会议时间里让总统对最重要的事情有所了解。[203]

和麦康奈尔一样，副总统切尼也需要做早课。清晨6点半左右，最新一期《总统每日简报》会送到他的官邸。通常情况下，他的办公室主任利比会和他一起阅读这份材料，简报员在一旁等候，并且随时准备回答问题。他的那份《简报》包含两个部分，第一部分跟总统的那份一样，第二部分是他曾经过问的情况，或者情报员猜测他会感兴趣的一些问题的回应，这一部分又被叫作“表格后面”。如果切尼认为“表格后面”的一些材料需要总统了解，他会把它抽出来放进第一部分。[457]

通常情况下，通气会只有极少数的几个人参加。除了国家情报总监或者先前设立的中央情报总监、小布什和副总统切尼，还有总统幕僚长和国家安全事务助理。如果事情复杂、事关重大，还要把情报分析人员请来，他们把这种情况叫作“深潜”，大概就是刨根问底的意思。在小布什准备进攻伊拉克的时候，就曾经组织过一次“深潜”，国防部部长和国务卿都参加了那次通气会。[203]

参加总统情报通气会的人都会拿到一份《总统每日简报》。有人说每期简报有10～15页[458]，也有人说是20～25页。[459]千万别小看了这份简报，它可是美国情报界非常有名、非常高端、非常引以为豪的一种产品。这份简报的诞生要追溯到1946年2月15日。这一天，一份叫作《每日要闻》的报告送到了杜鲁门总统手里。就从这一天开始，美国总统每天都会收到情报部门提供的概要报告。1951年，中情局设立了动态

情报室，专门负责出版《形势要闻》，这份情报刊物的内容与《每日要闻》类似，但一周一期，主要是作为中央情报总监向总统汇报最新情报的素材。动态情报室成立后不久，《每日要闻》就改名为“动态情报通报”，1958年再更名为“中央情报通报”，并且根据中情局总监察官的建议，这份刊物开始反映整个情报界的分析结论，而不仅仅是中情局的分析成果。1961年肯尼迪总统的幕僚要求情报通报文字更加简洁、印刷开本更加小巧，能够放进总统的口袋。三天后，《总统情报清单》就送到了肯尼迪的桌上，总统非常满意。到了约翰逊总统那里，这份情报刊物再次改名，这个名字从此以后再也没有改变过——“总统每日简报”，时间是1964年。[460]

2004年，随着最后一任中央情报总监把原先承担的“统管”和“协调”任务交给了国家情报总监，制作《总统每日简报》所需的协调工作也转移到了国家情报总监办公室。这份刊物反映了整个美国情报界的工作，被总统倚重，但内容主要还是由中情局的情报分析人员撰写。[460]

奥巴马把通气会推迟到9点半，前面描述的麦康奈尔总监起早贪黑赶“早朝”的那番情景便成为一段历史，后来的国家情报总监并非每次都出席通气会，大多数情况下由常务副总监代为参会。[459]和他的前任相比，奥巴马更加关注《总统每日简报》的传递形式。他要求下属研究一下如何通过电子形式传递这份刊物。[460]总统的这个命令得到了积极的回应，并且很快就有了阶段性的成果。2012年1月底，白宫御用摄影师苏扎上传了一张奥巴马聚精会神摆弄平板电脑的照片，据说当时他正在阅读《总统每日简报》。[461]有人开玩笑说，这个简报的App有可能是世界上最专用的一款应用程序。当然，为了安全起见，有关部门对奥巴马他们使用的平板电脑进行了专门处理，封锁了这些平板电脑上的无线功能。[462]

其实那个时候，简报还没有完全实现数字化，总统能够在平板电脑上读到的只是部分内容。[463]来自麻省理工学院林肯实验室和谷歌公司的技术专家大声疾呼完全电子化的好处、畅想完全电子化之后可以新增的功能，其实这些都是显而易见的事情。[464]就在他们的文章发表后的两个月，纸质简报最后的日子终于到来了，那一天是2014年2月15日。[460]从此以后，《总统每日简报》完全实现电子化，不再印行纸质版本了。

据熟悉情况的人士透露，小布什在任期间，每周召开6次情报通气会，这个规定几乎雷打不动。他还亲自主持过100多次“深潜”，直接听取情报分析人员的意见。奥巴马似乎不太喜欢这种面对面的会议形式，在他第一次当选后的1225天时间里仅召开过536次通气会，次数与天数比例大约是43.8%。2011年到2012年上半年，这个比例降到只有38%。[465]对此只有一种解释，随着时间推移，奥巴马更加依赖《总统每日简报》而不是通气会获取信息。而就是这样一种重要的情报产品，2011年有1152次引用了“棱镜”计划搜集到的数据，占信号情报总引用量的15%；2012年增加到1477次，所占比例增加到18%，简单计算一下，平均每天4次。这样一个比例在所有信号情报源中是最高的。[466]

“棱镜”计划的作用还不只是支撑《总统每日简报》。这里有几个数字，可以比较直观地了解这个计划发挥的作用。国安局内部平均每7份报告中就有1份会用到“棱镜”计划的数据[417]，平均每个月有2000份报告基于“棱镜”数据，2012年引用“棱镜”计划的数据的报告有24005份，比前一年增加了27%。[419]所以在斯诺登提供的“棱镜”计划幻灯片的封面上，负责的人不无得意地写道：“棱镜/US-984XN，国安局报告中最常用的信号情报行动编号。”

戈尔曼和格林沃德等人通过《华盛顿邮报》和《卫报》曝光“棱镜”计划后，原本深藏在幕后、处于高度机密状态的监视计划突然成为新闻媒体聚焦的热点和街头巷尾普罗大众的谈资，特别是对于它们的合法性、合理性以及监督审查问题，人们普遍存在质疑。国家情报总监汇聚整个情报界的力量打造的高端情报产品、当今总统极为倚重的重要情报源建立在这样的基础之上，必然受到严重影响。国家情报总监坐不住了，总统也坐不住了。面对记者的提问，奥巴马是这样为国安局的监视计划辩护的：

这些计划完全处于国会以及外国情报监视法庭的双重监管之下，这个法庭专门评估政府在秘密计划中是否有违反宪法和滥用职权的情况……

美国人民理解，（要顺利执行计划）需要一些代价。我对这些计划持积极的怀疑态度。我的团队对它们进行了评估。我们彻底检查过这些项目，扩大了监管范围，增加了保护措施。不过，我和我的团队对这些计划的评估意见是，它们帮助我们阻止了恐怖袭击……你们不可能在100%安全的同时保留100%的隐私，并且无任何不便。[467]

最后，他把前两天各媒体的热烈报道定性为一种“炒作”。但奥巴马的这番话，即便是他的盟友、民主党二号人物、党鞭理查德·德宾（Richard　Durbin）都表示难以接受。德宾指出，国会并不能实时了解项目的情况，只有一小部分高层领导人可以定期获得通报。总统说国会批准了这个计划，这话并没有错，但这种说法所暗示的信息通报和监管状况并不存在。[468]

奥巴马心里当然清楚，与之前的监视行动相比，“棱镜”计划以及“上游”计划所处的管理环境和约束条件要宽松得多。外国情报监视法庭只需要审批国安局等情报和执法单位开展监视行动的整体过程，重点是看看他们有没有设置内部审查机制，尽量保证监视目标“人”是不在美国的外国人，尽量避免“附带搜集”发生，这种机制被模模糊糊地定义为“最小化过程”。只要法庭认为有关单位建立了这样的机制，就会批准他们开展监视行动。而对于某个目标“人”是否应该被监视，以及对他监视期间是否发生了违法的情况等具体事项，不再追查。这些“细节问题”统统交给相关单位自己查、自己办。这种做法都处于《外国情报监视法案》（修正案）的允许范围之内。

在很多开明人士眼中，由于政府部门的互联网监视计划已经处于外国监视法庭的监管之下，这些计划就是合法的，并且受到很好的控制。[469]他们还想当然地认为：如果政府部门要检查美国人的电子邮件或者电话的内容，就需要得到法庭的调查令。[470]奥巴马总统对于秘密监视计划的辩护说辞更加坚定了他们的这种认识：

如果你是一个美国人，按照法律制度，国安局不能监听你的电话，除非他们从法庭那里获得调查令，从来都是如此……[471]

对政府充分信任的人们可能想象不到，精通法律的奥巴马总统所说的并不总是实际情况。法庭依据《外国情报监视法案》发布的调查令，监视目标及其被监视的理由必须是明确的。1978年颁布这部法案的主要目的就是，防止政府部门在没有法庭单独授权的情况下，对美国人的电子通信进行监视。而要得到这样的授权，有关部门必须拿出“相当的理由”，表明想要监视的这个人是国外特工或者恐怖组织成员。[472]

30年后出台的这部新法律只是标题上增加了“修正案”三个字，并且“巧妙地”规定，只要是针对外国人，准确地说是针对身处美国之外的外国人进行监视，可以不需要对具体监视目标发布调查令。之所以说

它“巧妙”，是因为从表面上看，它没有改变“对美国人监视就需要调查令”这样一个被美国大众普遍接受的常识，顺利在国会获得通过。实际上，由于监视目标不再由法庭审定，美国人完全可能在没有调查令的情况下被情报部门和执法部门监视。换句话说，这部新的修正案几乎完全颠覆了原来的那部法律。耶鲁大学法律教授杰克·巴尔金（Jack Balkin）评论说：

（这部新的法案）不再要求所有的监视计划都针对某些单独的目标。（也就是说，）由于这些计划并没有直接把美国人作为其监视目标，也就不再需要针对某个特定人发出调查令，它们可以像“吸尘器”那样运作，对大量的不同个人的通话进行监听、对大量的不同个人的电子邮件进行检查……

这部新的《外国情报监视法案》授权建立针对外国人的监视计划，或者说建立针对身处美国之外的人士的监视计划。这些计划不需要单独怀疑某个人是恐怖分子，或者参与了犯罪行动。这将不可避免地搜集到美国人的许多电话信息，尽管他们跟恐怖主义和“基地”组织毫无关联。[473]

巴尔金教授这里说的是针对电话信息的监视计划，但同样适用于针对互联网信息的“棱镜”计划和“上游”计划。依据新的《外国情报监视法案》（修正案），甄别某个人是否是美国人、是否身处国外这样的重要问题被当作“细枝末节”，交给了情报部门和执法部门。这样做的一个主要好处就是：情报搜集工作的效率可以大大提高。

数据，又是数据

《总统每日简报》中引用的“棱镜”计划的数据主要有两个来源：其一是存量数据，就是从已经存储的通信数据中筛选出目标“人”的信息；其二是新增数据，这要等待互联网公司从最新的海量数据中挑选目标“人”的信息。不难看出，无论从哪种来源获得数据，都需要设定一些筛选条件，也就是筛选点，这项工作只能由国安局的情报分析人员来做。他们把筛选点信息输入“目标锁定一体化工具”（UTT），同时说明筛选目的，并且写清楚为什么筛选出来的数据不涉及美国人以及身在美国的外国人。这些附加的步骤被赋予非常重要的意义，分别被称为“对外情报之目的性判定”（简称“目的性判定”）和“监视目标之外国性判定”（简称“外国性判定”），也是后面若干个内部监管节点审查的重点。

这两种判定之中，前面的“目的性判定”很简单，情报分析人员几乎总是直接打个勾就行了。后面的“外国性判定”稍微麻烦一点儿。对于这个问题，国安局在提供给外国情报监视法庭的文件上是这样描述的：

国安局判定一个非美国目标“人”身在美国之外，其依据是有关此“人”所有可以得到的信息，包括他使用的（各种）通信设施的信息。[472]

根据官方的解释，“设施”这个概念已经被扩展，不仅仅是电话、计算机这样的“硬件”，还包括电子邮件信箱、计算机账户等“软件”。绕来绕去，其实需要分析人员做的就是写上一两句话，比如说“该目标‘人’声称自己在国外”，或者“信号情报报告确认该目标‘人’在国外”。不难看出，这样的“外国性判定”结论多半是一些套话，已经被固化为菜单选项，所以大部分文字录入工作都由软件“代劳”了，分析人员需要做的可能只是点几下鼠标那么简单。国安局对情报分析人员的要求是，只要他们有51%的把握就足够了。[428]

不难看出，把“目的性判定”和“外国性判定”这两个重要问题完全交给情报分析人员，可以套用一句俗话，叫作“说起来重要，干起来次要，忙起来可以不要”。由于源头上的大而化之，后面的所谓“严格监管”的过程和措施便难免流于形式。

从存量数据里筛选目标“人”的信息，要经过四道关口。第一关是《外国情报监视法案》监管处（SV4），按照《大西洋月刊》特约编辑马克·安百德（Marc Ambinder）的说法，这个监管处是国安局内的一个部门；[474]第二关是数据搜集部目标锁定与任务管理处（S343）；第三关是“指纹氛围”（PRINTAURA）系统中的数据分发主管；按照《华盛顿邮报》的说法，第四关是联调局的电子通信监视部（ECSU），他们要在自己的数据库里检查来自国安局的筛选点信息，看看这些筛选点信息是不是属于某些已经被确定的美国人或者身在美国的外国人。[475]经过了这一关，他们才从存量数据中把目标“人”的信息调出来，并通过数据侦听技术部（DITU），把这些信息传递给提出需求的情报分析人员。

如果存量数据中没有找到目标“人”的信息，就需要从互联网公司那里获得他们的数据了，这也需要经过两道关口。情报分析人员所在的产品线都设有专门的审裁员，要让互联网公司监视目标“人”，必须得到这些审裁员的同意。这是第一关。和前面那种情况一样，第二关也是要由目标锁定与任务管理处批准。接下来由“指纹氛围”系统中的站点分配主管挑选合适的互联网公司，但国安局并不是直接跟这些公司联系，而是由联调局的数据侦听技术部代为出面，让这些互联网公司提供目标“人”的数据。如果在获取互联网公司数据时遇到了技术问题，也总是通过数据侦听技术部进行协调。例如，国安局在与微软公司“合作”的过程中发现，公司的Outlook.com网站允许邮箱用户创建别名（alias），这可能导致“棱镜”计划针对这些用户的任务设定产生问题，于是他们通过数据侦听技术部联络微软公司并且圆满地解决了这件事情。[433]

一旦互联网公司得到了目标“人”数据，这些数据就会通过联调局的数据侦听技术部进入“指纹氛围”系统。从这一步开始，下面提到的这些过程都发生在国安局内部。如果筛选点是电子邮箱，得到的元数据将进入“流量贼”（TRAFFICTHIEF）系统，这个系统是亚历山大局长主持建设的“动荡”项目产生的一项成果。[265]

其他需要处理的数据传入“剪刀”系统后，根据数据的类型进行分流，在国安局内部这项工作被称为“协议开发”。具体地说，语音内容数据和元数据分别进入“输送”和“争执”系统。《华盛顿邮报》说，这两个系统似乎是减少美国人数据被“附带搜集”的最后一道关卡。[475]除了语音内容数据和元数据，其他数据则需要再次通过“剪刀”系统。

最终，搜集到的数据将分门别类进入若干带有数据分析功能的系统：互联网元数据进入“小码头”、电话元数据进入“主干道”、语音内容数据进入“核粒子”、视频内容以及其他数据则进入“灯芯绒”。搜集到的数据处理完后，会自动传送至最初设定任务的分析人员那里。从设定任务到得到数据之间需要的时间快至几分钟，慢到几小时。[476]

需要说明的是，这一套看似复杂的过程，特别是“目的性判定”和“外国性判定”，并不局限于“棱镜”计划，“上游”计划中属于《外国情报监视法案》（修正案）第702条授权的那部分工作内容，也需要经过这样的程序。

看到这么多莫名其妙的系统代号，是不是有点儿糊涂了？的确如此。在这里，大部分代号都是第一次提到，并且到目前为止，有关这些系统更详细的情况还锁在国安局的保密柜里。

说实话，对于“棱镜”计划的任务设定过程和数据分流过程，仍然存在一些疑惑。这其中有一个关键词——“存量数据”。从幻灯片上看，这些数据存放在联调局，那么它们与国安局若干个数据分析系统里保存的通信数据是什么关系呢？

2012年班福德在《连线》杂志上发表过一篇文章，披露了国安局在犹他州新建的数据中心的一些情况。据斯诺登说，这个数据中心原本叫“海量数据仓储”（MDR），后来因为局里有些人觉得这个名字太过真实、有点儿吓人，改成了“任务数据仓储”[15]。

班福德提到的这个中心的数据大厅有10万平方英尺（大约9300平方米），可惜人们目前还不知道其存储规模。尽管如此，文章中还是数次提及“尧字节”（YB）这个概念，它表示10的24次方字节。这个数量级到底有多大？据思科公司估计，全球互联网的流量在2010~2015年将会翻四番，即便如此，每年的流量也还不到1000艾字节（EB），也就是不到千分之一尧字节。[477]换句话说，如果这个数据中心真的具有尧字节等级的存储能力，国安局完全可以把几十年甚至上百年整个互联网的数据流量都截取下来、保存起来。这样一种描述，自然让人对国安局的数据存储能力浮想联翩，也必然心生疑问：国安局要如此巨大的数据存储能力做什么呢？“棱镜”计划曝光后，班福德试图把监视计划和这个数据中心关联起来，不过他还是缺少关键的一根链条：国安局保存了哪些数据、保存了多少数据。[478]看起来“存量数据”应该是一个很有新闻价值

的问题，但似乎没有引起戈尔曼和格林沃德等人的足够重视。

国安局如此巨大的数据存储能力当然不会被浪费。仅仅2012年1～6月，每天转入“小码头”系统的元数据大约100亿条，而转入“手机盖”（FASCIA）系统的元数据大约50亿条。[479]也就是说，每年转入这两个系统的元数据大约就有5.5万亿条之多。这些都还只是国安局搜集到的数据的冰山一角。对于搜集到的数据，美国的法律从来都是内外有别、实行双重标准的。按照法律规定，“纯”美国数据原则上应该被彻底删除。例外的情况是，如果这些数据包含了“重要的外国情报信息”“犯罪证据”等，就可以申请保留。对于“附带搜集”的、可能涉及美国人的数据，由于国安局的“过滤能力不足”，可以在他们的数据库里保存5年。[480]针对这种做法的荒谬性，曾经为国安局提供过技术咨询的一位专家评论道：“这就相当于如果不能立刻淡化所有海水，就把整个海洋控制起来，直到找到解决办法。”[481]至于外国人的数据，估计可以长期放在国安局的数据库里，想存多久就存多久。

据国安局的官员介绍，他们在连接全球移动网络的电缆上搭线，获取了移动用户的大量定位数据，这些数据都进入了“手机盖”系统。说到搭线搜集数据，必然会想到“上游”计划。的确，给“手机盖”提供定位数据的配套计划有10多个，“上游”计划中的“锦绣镇”“橡木星”“风暴酿”都在其中，“防风布”“护城墙A”这样的跨国合作计划也在其列。除此之外，还有“绿洲舞”（DANCINGOASIS）、“潜修人”（MYSTIC）、“树林线”（TIMBERLINE）等陌生面孔。[482]说到“潜修人”计划，给“手机盖”提供定位数据对它而言算是小菜一碟，它的能力非常强大，足以百分百地保存某个国家的全部电话记录，还可以检索和回放一个月以来通话者的通话内容。[483]国安局为如此神奇的计划选择了一个白发魔法师的形象，他手中的魔杖上醒目地放着一部翻盖手机。

这么多计划的背后都有一个共同的名字——特情处。斯诺登对这个单位推崇有加，把它比作国安局“王冠上的宝石”。

“小神童”

特情处隶属于国安局信号情报分局的数据搜集部。除了特情处，在数据搜集部的下面还有一个非常神秘的单位，叫作“特接处”（TAO），就连在国安局里工作的很多员工也搞不清楚这个单位具体是做什么的。前面曾经提过，斯诺登刚到博艾汉公司的时候推掉了特接处的工作邀请，转而去了威胁行动中心。特接处负责的行动极为保密，没有几个国安局官员能够说清楚。想要进入国安局大楼里属于他们的办公区，需要特殊的通行许可。[484]说它“非常神秘”一点儿也不夸张。

第一眼看到“TAO”，中国读者可能会觉得很亲切。因为中国道家学说中的“道”翻译成英语就是“Tao”。但稍稍多了解一点儿这个“TAO”，它可就一点儿也亲切不起来了。因为，它是真正意义上的以黑客攻击作为主要任务的部门。真可谓此“盗”非彼“道”！

《外交政策》杂志在2013年6月刊登了艾德撰写的一篇文章，其中提到，特接处已经成为信号情报分局内部最大的一个部门，员工超过1000人，下面设置了若干个科或者中心，其中最重要的要算远程行动中心（S321，ROC）。[484]虽说斯诺登没有到特接处工作，他选择的那个威胁行动中心，主要负责赛博防御，与远程行动中心关系密切，有时候这两家单位还要协同工作。这样的工作性质也要求斯诺登熟练掌握各种黑客技术。[485]

几乎所有人在说到远程行动中心的时候，发音都和“岩石”（rock）相同。[485]在米德堡总部，他们的办公区戒备森严，门口有全副武装的警卫把守，想要进去，除了需要输入6位数的密码验证，还必须通过视网膜扫描仪检测。行动中心有600名军方和民间电脑黑客，他们把自己叫作“计算机网络开发操作员”，每周7天、全天24小时轮班工作。[484]

“计算机网络开发”（CNE）是一个既不惊人也不起眼的术语，看上去完全无害。但国安局前官员透露，这个术语在国安局内部专门用来描述下列这些事情：秘密入侵海外的目标电脑和电信系统、破解密码、攻破其电脑的安全系统、窃取其存储在硬盘上的数据、窃取其电子邮件和聊天消息。[484]经过“开发”的计算机和网络，就处于随时可以被国安局

袭击和攻克的状态。[485]

通俗地讲，远程行动中心的工作就是利用黑客工具进行网络扫描，发现网络和计算机中的漏洞，入侵目标网络和计算机系统，开展监视工作。他们需要的软件和硬件工具由特接处下属的四个技术部门提供。搜集数据所需的软件工具由数据网络技术科（S323，DNT）进行开发，而悄悄潜入目标网络和计算机系统的工具由通信网络技术科（S324，TNT）开发。[484]

相比之下，先进网络技术科（S322，ANT）看上去更神秘一些，甚至让人有点儿不知所云。他们的名字还可以翻译成“高级网络技术”，如果按照中国台湾地区的习惯，更可能翻成“进阶网络技术”，可以理解为建立在前面两种“网络技术”基础之上的一类技术。这到底是些什么技术呢？根据已经掌握的材料，“先进”一词，可以按照字面的意思理解，是指“先”采用手段，“进入”原本不联入互联网和其他通信网络的计算机和设备，把这些计算机和设备联入国安局构建的“网络”之中，接下来再用前面两种网络技术进行攻击。

任务基础架构技术科（S325，MIT）的任务比较明确，他们负责开发监控目标网络和计算机的硬件工具。获取技术行动科（S326，ATO）则主要负责“脱网”行动，中情局和联调局经常会派一些特工临时帮忙。[484]先进网络技术科设计的产品，总是要由特工部署和安装，因为这样的工作并非国安局的职责范围，需要协调中情局或者联调局的力量去完成。如果涉及海外任务，就可能需要特搜部帮忙了。

等监视设备安装到位，远程行动中心的黑客们就可以坐在米德堡的办公室里，从容镇定地开展监视工作。[484]不过要做好这项工作，还需要定期或不定期地告知自己的同行，特接处的技术部门已经开发出哪些新产品。这大概就是2013年12月《明镜》周刊曝光他们产品目录的由来。获取技术行动科的规模不大，这很容易理解，因为他们的工作主要就是联络和协调。

前国安局的官员曾说：特接处自己就是一种产业，他们去的那些地方、获得的那些情报是情报界的其他单位接近不了、也拿不到的。[484]看完上面的介绍，也就真正理解了这句话的意思。这个“产业”的确已经形成配套体系：先进网络、数据网络、通信网络和任务基础架构这四个技术部门负责技术开发类工作，形成黑客软件、黑客硬件等产品；

远程行动中心运用黑客软件开展窃听活动，得到情报；获取技术行动科负责协调中情局特工在海外安装黑客硬件，为后续的监视活动铺路搭桥。

特接处成立于1997年，说起来，在国安局内部只能算一个相当年轻的部门。尽管年轻却不容小觑。艾德说，他们就像美国情报界的“小神童”（wunderkind）。[484]仅仅10年后，他们已经秘密侵入成千上万的外国计算机系统、受密码保护的计算机硬盘以及目标人物的电子邮件账户，在他们的黑名单上有来自89个国家和地区的258个重点目标人物。[486]这个名单总是处于不断扩充和调整之中。墨西哥前总统费利佩·卡尔德隆（Felipe Calderon）和他的继任者恩里克·涅托（Enrique Nieto）都榜上有名。[487]国安局在2010年11月的一份报告中宣称：特接处在半年前成功“开发”了墨西哥的PRESIDENCIA邮件服务器，首次打开了卡尔德隆总统使用的公开邮箱。除了总统本人，墨西哥政府的其他内阁成员也在使用这个邮件服务器。这次代号为“平面液体”（FLATLIQUID）的行动成功，意味着美国人可以更好地洞察“墨西哥政治系统和其国内稳定的内幕”。[488]

特接处实施的“难住光标”（STUMPCURSOR）计划，在对伊拉克的军事行动中，帮助美军找到了100多名藏匿在巴格达附近的伊拉克和“基地”组织的“叛乱”分子。同样是在2007年，特接处还提供了特别重要的情报，帮助情报分析人员准确判断伊朗是否在建造核武器，并因此获得政府嘉奖。在国安局内部流传着这样一种说法：若想晋升被认可，那就快去特接处。由于工作成绩出色，特接处的前任处长特蕾莎·希亚（Teresa Shea）于2010年荣升信号情报分局局长。[484]

除了米德堡总部，国安局还在戈登堡建立了佐治亚分部，在圣安东尼奥的梅迪纳建立了得克萨斯分部，在瓦胡岛的瓦西瓦建立了夏威夷分部。特接处在国安局的这些分部都有自己独立的办公区。除此之外，丹佛城外巴克利空军基地的侦听站里也能看到特接处的存在。

得克萨斯分部最近几年的发展速度超乎寻常。2008年这里的特接处员工只有不到60人，计划到2015年达到270人，其中增长幅度最大的是远程行动中心，计划从37人增加到141人。[486]关于这个分部，在当地还有这样一个小故事。

2010年1月的一天，圣安东尼奥城发生了一件怪事。准备去上班或

者买东西的人们惊奇地发现，无论他们怎样摁动遥控器按钮，电动车库的大门都纹丝不动。这种怪现象主要发生在城市的西部。美国是“车轮上的国家”，没了车，他们寸步难行，神秘车库门问题迅速成为当地的政治问题，市政府不得不出面解决。一番调查研究之后，问题的原因很快就搞清楚了：“罪魁祸首”原来是国安局的得克萨斯分部。他们原本在拉克兰空军基地安家，2005年搬到了城市西部的一片废弃的索尼芯片厂区里，而他们的天线频率正巧与当地居民车库遥控器的频率相同。问题当然很快得到解决，而这个原本特别神秘的单位却露出了它的狐狸尾巴。[486]

“搜”“盗”二将

正所谓“无巧不成书”，按照他们的英文缩写，特接处（TAO）正合了一个“盗”字，而特情处（SSO）正合了一个“搜”字。这一“搜”一“盗”撑起了国安局信号情报搜集工作的半壁江山。《纽约时报》刊登过一张得克萨斯分部情报搜集渠道统计图，时间跨度是2009年11月30日到12月6日。这张图上显示，在这一周的时间里，整个得克萨斯分部的情报源有103个，其中特接处有6个，特情处有45个（包括通过《外国情报监视法案》（修正案）授权的24个情报源），两个单位加起来一共51个。[489]这张图虽说不够全面，但也从一个侧面反映出“搜”“盗”二将在整个国安局情报搜集工作中的地位和作用，“半壁江山”绝非虚言。

对于特接处的价值，希亚处长是这样说的：“情报的重要性不在其数量而在其质量。”[486]她说这句话时颇有些底气，因为特接处为政府提供过某些最为重要的情报，并且还不断从最“硬”的目标那里拿到情报。局里给特接处设定的目标是“拿到那些不可能拿到的情报”。不过她的这番话又多少透出一些“酸味”，在数据搜集部下面的另一员“大将”——特情处听来甚至有些刺耳。很明显，特情处的搜集工作明显带有涉及面宽、数据量大等特点，他们的徽标图案是一只白头鹰抓住了维系地球的数根电缆。这个单位最初起家就是从通信电缆搭线监听开始的。“吃水不忘挖井人”，时至今日，特情处仍然把自己的情报搜集工作统称为“电缆计划”，尽管其中包含的内容有一些可能已经跟通信电缆没有一点儿关系了，比如“棱镜”计划。

总的来看，特情处的搜集计划分为三大类，第一类是与本国公司合作，主要包括“棱镜”计划以及上游的“布拉尼镇”“锦绣镇”“风暴酿”和“橡木星”计划；第二类是跟国外的伙伴合作，主要包括“防风布”计划和“护城墙A”计划。关于最后一类计划，目前只公布了五个计划之中的三个，分别是“护城墙I/X”“护城墙T”以及“潜修人”计划，这些计划的特点是行动主体只有一个，就是特情处自己。上面提到的这些计划，大多数在前面已经介绍过。剩下的两个被涂黑的计划到底是什么，无疑是一个值得探究的问题。

网上有人指出，在特情处的各个搜集计划中，如果按照搜集到的数

据量排名，排在首位并且遥遥领先的并不是上面提到的这些计划，而是代号为“绿洲舞”（DANCINGOASIS）的搜集计划，其行动编号为“US-3171”。这个计划在一个月内搜集到的数据就有578亿条之多，占到特情处总搜集量的1/3以上，排名第二的“吐丝器”（SPINNERET）和第三的“月光径”（MOONLIGHTPATH）同属于“护城墙A”计划，它们俩搜集到的数据加起来大约有382亿条，仍不如“绿洲舞”多。所以，被涂黑的两个独立进行的计划里，有一个很可能就是“绿洲舞”。

在更多情况下，特情处也好、特接处也好，信号情报分局下的这两员“干将”在重大任务面前，一“搜”一“盗”，互为补充，分别发挥自己的专业特长，为国安局增光添彩。2010年春，联合国安理会即将投票表决对伊朗制裁的决议，当时的美国驻联合国大使苏珊·赖斯给国安局布置了一项重要任务：尽一切可能获取联合国主要成员国在投票意图方面的情报，以便争取主动、获得优势。[466]国安局对此高度重视，具体任务主要还是落在了这“搜”“盗”二将身上。

对特情处而言，时间紧、任务重，参与这一任务的“布拉尼镇”计划小组四面出击：负责行动的人员在拿到法庭申请手续之前，不等不靠，加紧搜集有关数据，以便尽早确定能够从联调局那里获得哪些信息；负责目标的人员努力搜集有关国家驻联合国使团以及驻美大使馆的各种信息，确保数据流通畅、获取到的情报能够尽快传递到需要的人手中；负责法庭申请手续的人员以破纪录的速度在一天之内拿到了国安局局长、国防部部长和外国情报监视法庭法官的签字。[466]

相比之下，特接处就要气定神闲得多。因为他们的人员早就渗透进了许多国家设在美国的外交机构。在这次对伊朗制裁决议谈判的过程中，美国人最关注的是法国、日本、墨西哥和巴西的情报。在法国驻联合国使团那里，特接处已经采用“工具植入”和“屏幕信息捕获”两种搜集手段进行了渗透，行动代号为“黑脚人”（BLACKFOOT）。他们的这两种搜集手段也有代号，分别被称为“高地”（HIGHKANDS）和“游民”（VAGRANT）。而对于盟国日本，美国人其实并不放心，在他们驻联合国的使团那里，除了上述两种手段，特接处还采用“电磁泄漏传感器捕获”和“局域网工具植入”进行渗透，这两种搜集手段也有代号，分别叫作“磁铁”（MAGNETIC）和“矿化”（MINERALIZE），他们还给对日本使团进行的监视行动起了一个名字，“桑葚”（MULBERRY）。[466]

最终联合国的这项决议以12票支持、2票反对（巴西和土耳其）、1

票弃权得以通过。赖斯事后夸奖国安局说，信号情报透露了常任理事国在制裁问题上的真实立场，揭示了有关国家的谈判底线，帮助她掌握了哪些常任理事国在说真话，得以确保美国在谈判中始终处于上风。[466]可以说，这是对国安局信号情报工作成绩的最高褒奖，这种成绩的取得，“搜”“盗”二将功不可没。

千万不要认为这次针对伊朗制裁决议谈判的监视行动，是国安局第一次在联合国进行的监视活动。早在1945年4月决定建立联合国的旧金山会议上，国安局的前身、美国陆军信号安全局就承担过类似的任务。那时，欧洲的战火刚刚熄灭，日本法西斯还在负隅顽抗，“二战”尚未完全胜利。根据战时审查的法律要求，各大电报公司都必须把加密或者非密的电报交给信号安全局。即便是他们的盟友法国代表团，也处于严密的监视之下。代表团与巴黎之间的往来加密电报都被截获，而他们使用哈格林电报机发送的消息，信号安全局在若干年前就可以破译。[490]如果把这次旧金山会议比作一场牌局，那么自始至终，美国人都能看到对手手里的牌。这样一种始终占据上风的局面，也就成为几十年来美国人希望一直保持下去的理想状态，对联合国进行监听，自然就成为一种习惯性动作。

就在几年前，特接处还主要依赖一些比较低级的手段实施植入工作。比如，直接在物流过程上做文章，如果某个目标“人”订购了一台新的计算机或者其他设备，特接处会在中途把这些设备截获下来，运到他们自己的秘密加工车间，等在那里的特工们将小心翼翼地打开包装，把黑客软件植入进去，或者把黑客硬件安插进去。接下来，远程行动中心的黑客们就可以在自己的电脑前，静静地等待这些黑客硬件和软件悄悄打开系统的后门，然后神不知鬼不觉地进行“计算机网络开发”。在特接处的字典里，这种方法被叫作“供应链封锁”[486]，它也被认为是特接处最富成效的工作手段之一。[466]

此外，特接处还使用一种类似于“流氓”的做法——向目标计算机发送垃圾邮件，这些邮件里都附带恶意链接，如果不小心点到这些链接，浏览器就会访问特接处预先建立的特殊网站，在这些网站上针对不同浏览器准备了不同的“陷阱”，一旦浏览器转到这些网站的页面，黑客程序就顺利植入了目标计算机。这种手段相对简单易行，不过它也有一个不足：成功概率不高[486]——绝大多数人看到垃圾邮件都是一删了之，很少有人会打开这些邮件，那些预留的“陷阱”也就多半被闲置、发挥不

了作用。

如今，特接处的技术手段已经升级换代，他们开发了一组新的工具，由于这个新的工具包中的工具远远超出了原先的那些手段，它被命名为“量子理论”（QUANTUMTHEORY），大概是想反映出其效果的“跃迁”吧。在一张国安局内部的幻灯片上写着：“某些‘量子’任务的成功率高达80%，而垃圾邮件任务的成功率不足1%。”[486]这的确是一种“跃迁”。

“量子”任务首先需要特接处搜集到有关目标“人”足够多的数据，以便情报人员掌握他们的习惯。一旦做到了这一点，特接处就进入攻击模式，依靠“量子”工具包完成任务。等到带有某个目标“人”特征的数据包流经处于国安局监视之下的电缆或者路由器，“量子”工具包会自动判断目标“人”打算访问的网站，并且对该数据流进行重新定向，从网站回来的数据并不直接传到目标“人”那里，而是先经过国安局的专门服务器，在这些服务器上数据包被“改装”，植入黑客软件，之后专门服务器才把这些“加料”数据包发回到目标“人”的计算机上。[486]在讲解“量子”任务原理的幻灯片上，雅虎公司再次出现，这又一次印证了收服这家公司对于国安局情报搜集工作的重要意义。不难看出，“量子”方法基本上就是“供应链封锁”的网络化版本。

特接处给植入的黑客软件起名为“狐狸酸”（FOXACID），在一张内部幻灯片上，他们对这个代号给出了一种直观的解释：即使像狐狸般狡猾的对手，也可以用这样的强“酸”溶解掉。顺便说一句，监视网络设备的工作主要由特情处完成。也就是说，“量子”任务的顺利完成有赖于“搜”“盗”二将的紧密配合、大力协同。

不过，特情处也并不总是“彬彬有礼”地搜集，有时，他们做起事情来和特接处相似，也像个“黑客”。比如，他们秘密地破解了连接谷歌和雅虎公司数据中心的通信线路，大量窃取存储在这些数据中心的用户数据。国安局在2013年年初的一份材料里说，他们每天从雅虎和谷歌公司的数据仓库里窃取并且传输到米德堡总部的数据记录有数千万条，30天内新入库的数据竟达到1.8亿条之多，其中不仅有元数据，还有文本、语音和视频等内容数据。[491]

为了防止数据丢失、保证不间断服务，谷歌和雅虎公司在世界各地建立了若干数据中心，这些数据中心之间用高速宽带光纤连接，定期进

行数据同步、数据备份。这样即使某个数据中心出现问题，整个系统也不会崩溃，用户的数据也不会丢失。而为了做到这一点，两家公司投入巨资，购买和租用了上千公里的光纤，努力确保数据中心之间的通信快速、安全和可靠。[491]

这么说吧，数据中心是谷歌和雅虎公司的命门。以谷歌公司为例，他们的数据中心就像一个堡垒，进出其中的人员控制非常严格，中心还配备了热敏摄像头、生物识别装置，进行24小时不间断地监控。可即便如此，他们极为重视的这些东西还是被特情处找到了薄弱环节：用户访问这些公司网站的时候，提供服务的是“前端服务器”，采用的是保密性比较好的“安全套接层”（SSL）协议，但是，这些前端服务器与后端的数据中心之间，以及不同的数据中心之间通信时，没有采用高水平的加密协议进行保护，如果对这些通信线路进行监视，就能易如反掌地拿到公司的用户数据。[491]

谷歌公司察觉到了这个问题，正在加紧研究，准备尽快加以解决。但他们没想到利用这个问题做文章的竟然是国安局，因为他们在心底对国安局还是抱有一些幻想的：一方面公司对“棱镜”计划的要求积极配合，基本上做到了有求必应；另一方面，就在不久前，亚历山大局长还亲自写信，邀请公司的创始人之一布林（Sergey Brin）和总裁施密特（Eric Schmidt）参加高层会议，专门讨论移动设备的安全问题。[492]简而言之，谷歌公司感觉自己与国安局之间的关系是相当不错的。所以他们在“棱镜”计划曝光之后发表了一份声明，“义正词严”地写道：

美国政府没有直接或者说通过“后门”访问我们数据中心存储的信息……我们只遵照法律要求向政府提供用户数据。[493]

谷歌公司的一位高管也拍着胸脯说：“根本没有把数据交给国安局的后门，一切都是通过前门进行的。他们给我们发来法庭指令，我们必须依法执行。”[494]他们多半想象不出，国安局竟会在如此和谐的关系中在自己背后捅上一刀。在这张高度机密的幻灯片上，特情处的技术人员还随手画上了一个笑脸，表达自己攻克谷歌安全堡垒之后的喜悦心情。攻破谷歌和雅虎公司的私用线路窃取数据，其实只是国安局“盟友未必是朋友”这句箴言的商务版而已。[491]

要知道，国安局是不能在美国国内偷偷搭线监视谷歌和雅虎公司的私用线路的，因为美国法律不允许他们这么做。但他们显然没有被难倒

——上有法律、下有对策，国安局找到了自己的老朋友，也是老搭档：英国人。

第七回 好搭档

这是格林沃德一行到达香港后的第7天。格林沃德更加忙碌，除了和报社联系、修改文章，他还要不停地接受采访，并且尽可能在斯诺登那里多待一会儿。他只能把每天的睡眠时间压缩到最少。相比之下，斯诺登的生活看上去很平静、很规律，每天晚上都能睡7个半小时。每次和大家分手，他都会轻松地说“我要回去睡觉了”，第二天再精神饱满、焕然一新地出现在众人面前。[276]

这一天，格林沃德猛然想起那个曾经跟自己联系过的“辛辛纳图斯”，这个神秘人物那里会不会也有什么重要的事情可以曝光。想到这里，格林沃德立刻开始寻找他的联系方式。邮箱里已经堆满了来自各方的邮件，其中有很多从来没有打开过。自从发表了第一篇有关威瑞森公司的文章后，他原先阅读所有来信的习惯就彻底改掉了。好在现在可以用关键词检索，格林沃德终于找到了辛辛纳图斯的账号，他马上给这位神秘人写了一封简短的邮件：

嘿，告诉你一个好消息。我终于用上了PGP电子邮件了，尽管这件事花费了我不少时间。如果你还有兴趣，我随时可以跟你谈谈。[276]

没过多久，他和波伊特拉斯按计划见到了斯诺登，没想到见面后，斯诺登幽幽地说了一句：“你刚才发邮件的那个辛辛纳图斯，他就是我。”听到此话，格林沃德半晌才反应过来，这实在太出乎他的意料了。[276]

走上前台

“那些以牺牲自由换取安全的人既不配得到安全，也不配享受自由。”

面对镜头，斯诺登缓缓地背诵出本杰明·富兰克林（Benjamin Franklin）的这句名言，作为访谈的结束语。这是他在这家香港酒店的最后一夜。他知道，从这一夜开始，他将彻底告别过去，踏上一条未来无法确定的人生之路。对他而言，富兰克林的这句话有着一种特别的、强大的力量。他更清楚，走到台前告诉世人自己的身份，意味着之后他必须立刻转入地下，开始逃亡生活。[371]

从《卫报》刊登针对威瑞森公司的法庭密令的那一天起，人们就开始猜测，给这家报社提供线索的是什么人，他手里竟然掌握着密级程度如此之高的文件。有些资深的圈中人已经嗅出了非同寻常的气息。他们自然而然地拿几年前的“曼宁事件”与现在的状况做比较。虽然曼宁通过维基解密公布的文件数量可观，但密级程度普遍不高，其中只有大约6%属于机密文件。[495]这一次则不然，接连报道出来的文件都是绝密，反映出来的内幕层次非常高，而且做法也完全不同。曼宁是直接把拿到的文件交给了维基解密，而维基解密把这些文件一股脑儿都放到了网上，没有加入新闻记者的梳理、分析和报道，其实普通人根本摸不着头脑。由于公布之前维基解密未对文件进行处理，尽管保持了原汁原味，但也给文件涉及的相关国家的安全带来威胁。而这一次曝光完全是通过主流媒体，对材料进行了解读，同时兼顾了国家安全的需要。相比之下，这种做法更为高明，也更为可取。

这位聪明的神秘线人到底是谁，一时间众说纷纭。住在香港一家酒店里的斯诺登则稳坐钓鱼台，有条不紊地安排自己的生活起居、按部就班地实施自己的计划，走向前台是他从一开始就设计好的。他曾对格林沃德说：“我不想隐瞒自己的身份，因为我知道我没有做错。”[495]

格林沃德第一次采访斯诺登的时候，波伊特拉斯就站在他身后拍摄录像素材。在格林沃德为文章的刊发时间表而着急上火的那段时间里，她主要忙着剪辑这些素材。不过，波伊特拉斯很快就发现，自己拍摄的

这些材料过于冗长琐碎、不太好用，不如重新拍摄。于是她设计了20多个问题，还是由格林沃德提问，进行了第二次录像。[276]

平时在酒店房间里，斯诺登总是穿着休闲T恤。这一次，格林沃德让他换上了正式一点儿的灰色衬衫，并且改坐在椅子上，身后放了一面镜子，使得狭小的房间看上去显得略微宽敞一些。面对记者的摄像机，斯诺登虽然是个新手，却表现不俗，流畅地回答了每个问题，思路清晰。站在一旁观察录像过程的麦卡斯基尔认为，斯诺登很上镜，他在镜头中的形象比他本人更好。[495]

这一回，波伊特拉斯很快就把采访录像剪辑成一段17分钟的视频。根据格林沃德和麦卡斯基尔提出的修改意见，她把视频压缩到了12分钟左右。可接下来波伊特拉斯就碰到了问题：三个人都不知道如何把这些视频安全地发回报社。得知这一情况后，《卫报》美国分社马上派计算机技能高超的网络版编辑戴维·布利申（David Blishen）飞往香港。布利申就出生在香港，而且他曾经和麦卡斯基尔在同一家苏格兰报社一起工作过。麦卡斯基尔让布利申把手机留在酒店前台，然后带他出去“散步”。走到外面，麦卡斯基尔才开口说正事。直到这时，布利申才知道自己这次来香港的真正任务。最终，他拿到了一张小小的存储卡，上面存储着斯诺登的采访视频。[495]

回到酒店，布利申马上就跟其在纽约的同事取得联系。他先是通过安全连接方式把视频上传到了一个加密的网络文件夹里，再把密码单独发了过去。可是没想到，美国方面居然打不开这段视频。无奈之下，布利申决定赌一次，仍然是通过安全连接方式，但不对文件加密，把视频发了过去。这实在有些冒险，因为他们的对手国安局是有可能截获这个视频的。好在这一次纽约那边终于拿到并且打开了斯诺登的这段视频。[495]

2013年6月9日，《卫报》美国分社网站上登出了格林沃德、麦卡斯基尔和波伊特拉斯三人合写的文章，随文章一并发表的还有这段珍贵的视频，正式向世人揭晓答案。他们在文章中写道：

美国政治历史上最重要的一次曝光的责任人名叫爱德华·斯诺登，29岁，中情局的前技术助理，现在是国防承包商博思–艾伦–汉密尔顿公司的雇员。最近4年，斯诺登一直在为国家安全局工作……

他在提供第一组文件的时候，附带了一份备注，上面写道："我明白，我将因为自己的所作所为承受痛苦。我深爱的这个世界正被一个由秘密法律、不公平的豁免和无法抗拒的权力组成的联盟统治着。如果我能够揭露这个联盟的作为，哪怕只是很短的一瞬，我都会感到满足。"

他认为，自己最好的出路是政治避难——有着"互联网自由冠军"美誉的冰岛是他的首选。他也知道，这个希望可能实现不了。

通过这一周的报道，整个事件引起了激烈的政治争论。（他说，）"我很满意，自己所做的一切都很有价值。我无怨无悔。"[293]

大约一个小时之后，视频报道的后续效应像火山一般喷发了：几乎每个电视频道都开始播放斯诺登的这段影像，美国有线电视网甚至不加删减地播出了整段视频。这也成为《卫报》有史以来点击率最高的一条新闻。斯诺登招牌似的形象从此为人熟知，而一些极为细心的记者已经根据他身后的灯具认出了他居住的酒店。[495]

斯诺登必须尽快离开香港。在当地人士的帮助下，斯诺登遁入了茫茫人海。几天后，格林沃德也离开了香港，一番思量之后，他没有在美国转机，而是经迪拜回到了巴西。[276]6月15日，波伊特拉斯被美国有线新闻网的记者撞见，面对提问，她拒绝回答、悄悄溜走，当天晚上，她就离开香港，直飞柏林。[354]

“示范性销毁”

斯诺登宣称，离开格林沃德等人的时候，他身上已经没有更多关于美国政府的秘密资料了。从后来发生的事情来看，他说的这句话是真的。那么资料到哪里去了？格林沃德和波伊特拉斯那里当然有很多，甚至有可能是全套资料。戈尔曼手里看来也有不少，他的主要阵地是《华盛顿邮报》。接下来就是麦卡斯基尔了。斯诺登把所有涉及英国的秘密文件都拷给了他，由这位“老”记者带回纽约。最终，拉斯布里奇总编带着这套英国文件的一个拷贝，回到了《卫报》的伦敦总部。[15, 496]

拉斯布里奇非常清楚，如果英国政府知道《卫报》手里掌握了这些文件，他们可以拿出英国法律，让法官立刻发布禁令，禁止报纸刊登此类材料，同时要求报社立刻返还所有文件。报社当然可以申辩，但最好的结果将是，报社被卷入一场漫长且代价高昂的官司。打官司本身当然需要支付高昂的费用，更糟糕的是，在打官司的这段时间，《卫报》将不能报道这些文件里的任何内容。一场官司拖上几年很是普遍，如此算来，报社的损失就太大了。[497]因此，有关这些文件的事情，成为报社那段时间里的最高机密。

总编在报社大楼里开辟了一间小小的工作室，他自己把这间屋子叫作“地堡”。所有的窗户都用纸糊上，门口专门派了一名警卫24小时值班。警卫手里有一份名单，上面的人数非常少，只有名单上的人才可以进出“地堡”。手机一律不允许带进去，它们被要求放在门外的一张桌子上，每个手机都贴了一张纸条，上面写着主人的名字。房间里放了5台新买的计算机，从来没有连接过互联网，并且与一切网络保持“物理隔离”。斯诺登文件都放在加密的文件夹里，访问这些文件夹需要三个密码，没有人知道一个以上的密码。房间里还放着一个碎纸机。[407, 497]

尽管斯诺登在逃亡，对国安局机密的曝光却一天也没有停止，而且人们发现，有关英国情报机关开展监视行动的报道多了起来，《卫报》是揭露他们的主力。

2013年7月20日，这是《卫报》历史上值得永远记住的日子。

在《卫报》英国总部办公楼的地下室里，在英国政通局（GCHQ，政府通信总局）两名技术专家的监督和指导下，报社的三名员工头戴防护面罩，手里拿着角磨机、电钻机，把计算机的主要部件一块一块弄碎，报社的几位主管在旁边观看。两位技术专家还专门背来了一个消磁器，电脑的碎块被扔进消磁器里，最后是一声巨响，数据终于被彻底销毁了。两位负责监督的政通局技术专家用手机拍了照片，算是留下证据，最后，他们拎着大包小包在伦敦买好准备带给家人的礼物，离开了报社。[497]

英国政府把这次活动称为“示范性销毁”，被销毁的就是拉斯布里奇手里掌握的斯诺登文件。

一个多月前，在格林沃德有关“棱镜”计划的文章发表后的几个小时之内，《卫报》又发表了记者尼克·霍普金斯（Nick Hopkins）撰写的一篇文章，指出英国政通局也从“棱镜”计划中受益。其中写道：

（政通局）2012年利用“棱镜”计划获得的数据，编写了197份情报报告——这一数目比前一年增加了137%……多数互联网大公司都在美国，处于英国司法管辖权之外。要从这些公司那里获取数据，英国政府部门需要走正常的法律程序。

由于英美两国之间有法律援助协议，政通局可以向美国司法部提出申请，由他们帮助自己获取数据。尽管这种方法运用得非常广泛（仅2012年，政通局就针对谷歌公司的数据提出过3000次申请），但这种方法需要的操作时间很长。看起来，“棱镜”计划给政通局提供了绕过这些法律程序的一种途径。[498]

这样一条消息当然让英国政府不太高兴，但还没有达到让他们感到窘迫的程度。他们立刻采取一些补救措施，以政通局的名义，给新闻媒体下达《国防咨询通知》，试图通过这种特殊命令的形式阻止英国国内媒体进行相关报道。这份通知不仅发给了《卫报》，还发给了英国广播公司（BBC）、天空电视台等各大媒体，提醒各媒体不要跟进报道《卫报》美国分社报道“棱镜”计划的内幕消息。[497]这份标记为“秘密”的通知是这样说的：

最近有许多报道，涉及英国情报部门从国外情报源获取信息的若干途径。尽管这些文章还没有违反国防咨询通知系统规定的原则，但就这

一话题继续讨论下去将对国家和相关人员安全造成威胁，情报部门对此十分关切。[499]

绝大部分英国媒体都表示将遵守通知精神——除了不太听话的《卫报》。所以，这段时间出现了一个非常奇怪的现象，当全球媒体广泛报道“棱镜”计划的时候，他们的英国同行按兵不动，几乎没有什么报道。[497]

几天后，《卫报》又根据斯诺登提供的文件，报道了政通局曾经两次在20国集团伦敦峰会上对英国的盟友进行监听。他们运用的手段主要包括建立专门的网吧，把参会代表上网时的一举一动全都记录下来，破解他们的黑莓手机，侵入他们的电子邮箱等。[500]文章发表的时间就像是提前安排好的：由英国举办的八国集团峰会将于文章发表的次日正式开幕。人们不禁产生联想，政通局会对这次峰会进行监听吗？[497]

英国政府终于有所反应。除了与总编拉斯布里奇通话，政府的两位高级官员还专门跑到《卫报》办公室，首次明确要求报社立刻交出他们手里的斯诺登文件。他们态度和气地跟总编和副总编说，这些材料是被窃的，报社不能拿它们做文章。他们还提到了《官方保密法》。这是政府手里最厉害的一件武器，其中规定，如果不是为了公众利益，记者泄露情报信息也是违法行为。不过两位官员只是亮出了这件武器，还没有真正打算使用它。他们表示，政府更愿意私下解决，而不是与报社对簿公堂。《卫报》方面则强调，迄今为止仍不知道其规模的政府监视行为，以及他们与技术公司和通信公司之间的合作关系，涉及侵害重大的公众利益，特别是所有这些政府行为当前明显缺少议会和司法监督。对这些事情进行揭露，符合《官方保密法》的要求。[501]

傲慢的政府官员显然没有听出报社方面的话外之音。不过，报社方面也并非一味表现强硬，他们表示，愿意在今后的报道中与政府加强联系。很快，又一篇重要的文章准备好了。拉斯布里奇明白，这篇文章的分量很重，前面的文章相比之下都只能算是餐前甜点。他主动向首相的新闻官提出建议，在文章发表前召开一次电话会议，避免这篇文章危害国家安全。几天后，首相派内阁秘书长杰里米·海伍德（Jeremy Heywood）到报社与相关人员面谈。但这次会谈没有按照《卫报》的预期进行，即讨论文章的关键细节以避免危害国家安全。海伍德希望的是根本不发表这篇文章，但他两手空空，没有任何具体有力的理由，也就根本说服不了报社。拉斯布里奇则告诉他，英国政府单方面的行动是徒

劳的，因为斯诺登文件现在保存在若干个地方，除了《卫报》，还有一些文件在好几个非英国政府的司法管辖区。比如说格林沃德，他现在身在巴西。这样的会谈当然不可能有任何结果。[497]

6月21日，这篇非常重要的文章最终刊登出来，它的关键词有两个："掌握互联网"和"时代"（TEMPORA）计划。随后《卫报》接连刊登了几篇揭露"时代"计划的文章。英国政府最终暗下决心，准备出手。

7月12日，海伍德再一次来到报社，和他一起来的是首相的新闻官奥利弗。他们告诉总编，《卫报》必须返还他们手里的政通局文件。海伍德说："我们很清楚你们手里有什么，也就只是三四十份材料。然而我们很担心这些文件的安全。"他还说，"这件事我们可以愉快地解决，否则我们将诉诸法律。"拉斯布里奇说，《卫报》不打算交出文件，"我们正在研究这些材料"。为了文件安全，政通局可以派技术专家来指导报社工作人员正确的操作方法。不过，他也做出妥协：报社可以在适当的时候销毁这些文件。[497]

又过了几天，卡梅伦首相的副国家安全顾问罗宾斯给拉斯布里奇打来电话。罗宾斯说，一切都结束了，部长们需要确保斯诺登提供的文件已被销毁。

拉斯布里奇：这没有道理。这些文件在美国人手里。我们也将继续从美国进行报道。你们将失去对事态任何意义上的控制。你们不会与美国的新闻机构进行这样的对话。你是不是在明确表示，如果我们不交出文件，你们就关停我们的报社？

罗宾斯：是的，我就是这个意思。

英国政府心里可能很清楚，砸毁报社机器只是一场"示范性"闹剧，并没有太多实际意义。但他们必须这么做，这就是英国人的行事风格。

拉斯布里奇当然不会坐以待毙。

当他还只是一个15岁少年的时候，拉斯布里奇就阅读了奥威尔文集，并立志长大之后做一名记者。后来他如愿考进剑桥大学学习英国文学，其间他还在当地的一家新闻媒体实习过，毕业后顺利地成为这家媒体的记者。三年后，26岁的拉斯布里奇就开始为《卫报》工作。从那以后的30多年时间里，除了很短一段时间在其他媒体单位当评论员、做分

社主编外，他一直在这家报社工作，从一名普通记者一步一步成为总编。熟悉他的人认为拉斯布里奇骨子里是个怀疑主义者，但却表现得像只水里的鸭子，看上去游得很平静，水面下的脚掌却在拼命划。[407]

对于《卫报》未来的发展，拉斯布里奇头脑里有着清晰的路线。在内容特点上，他希望这份报纸以调查报道为人所知。他刚一上任，就组织记者对英国内阁大臣艾特肯进行跟踪报道，《卫报》记者发现了一个重要证据，证明艾特肯编造了一系列谎言，这位大臣最后因为做伪证被捕入狱。这只是拉斯布里奇做的几件“大事”中的一件。2009年，《卫报》围绕默多克新闻集团丑闻的密集报道轰动一时，该事件以默多克关闭《世界新闻报》才算告一段落。2010年他领导报社对维基解密进行报道，着实让他的报纸又风光了一把。[407]这一系列新闻报道，加上这次对斯诺登文件的出色报道，《卫报》目前的在线读者数量已经是2009年的3倍，其中2/3的读者来自英国以外的国家或地区。

在报社的技术特点方面，拉斯布里奇心里早就有了目标：现代化、网络化、数字化。1993年的硅谷之行给他留下了深刻的印象，他在一份备忘录中写道，互联网就是未来，它将改变一切，我们必须用好它。报社大规模招聘年轻记者、改用彩色版面，把大量资源投入报纸的数字化在线版本，并且积极开拓美国市场。前文曾经提过，《卫报》美国分社实现了完全数字化运作，根本不出版纸质报纸。根据英国政府的统计数据，月访问量达4800万次的《卫报》网站是世界第三大英语报纸网站，仅次于《每日邮报》和《纽约时报》。[407]对于《纽约时报》，各位想必非常熟悉，而《每日邮报》则相对比较陌生。他们最擅长发掘各类八卦消息和刊发精美图片。斯诺登在世人面前亮相之后，《每日邮报》主要的报道对象就是他的女友米尔斯以及他在夏威夷的浪漫生活，同时还刊发了不少米尔斯在自己的博客里留下的香艳照片。[333]

这次，在公布斯诺登身份的那一天，《卫报》网站的日访问量达到了创纪录的700万人次[407]，在一周时间内，通过计算机和各种移动设备访问《卫报》网站的美国用户数分别增加了41%和66%，报社网站的美国点击量历史性地首次超过了英国点击量。[368]美国分社的互动栏目编辑组还和麦卡斯基尔合作，制作了一期题为“解密国安局档案”的互动式专题，详细介绍了国安局的大规模监视行动，把文字、交互式图表和嵌入式视频结合起来，形式非常新颖。[502]格林沃德、国安局前官员德雷克、参议员怀登、Lavabit创始人列维森以及国安局前法务长斯图

尔特·贝克尔等人悉数登场。当他们位于屏幕的中央时，其图像立刻就活了过来，滔滔不绝地向人们诉说，而当页面移动，他们就处于休眠状态。[503]

随着斯诺登文件的曝光，《卫报》吸引了无数眼球，也给自己带来了前所未有的压力。总编拉斯布里奇面临的考验也是前所未有的，他所能做的就是多几手准备、以防不测。考虑到“时代”计划的那篇文章可能出现问题，他通过联邦快递给某个中间人送去了一个包裹，里面有一个小小的U盘，装着挑选过的若干份斯诺登文件。这些文件最终被送到了独立新闻网站“为了人民”那里。网站的创始人保罗·斯泰格（Paul Steiger）原本是《华尔街日报》的编辑，他运营的这家网站曾经两度获得普利策奖。万一《卫报》遭到管制，不能发声，斯泰格将会在自己的网站上发布这些文件。[407]除此之外，网站还派了一名技术记者临时加入《卫报》的报道队伍，增强这支队伍的技术能力。这位记者具有很好的计算机学科背景，擅长解释复杂的数据挖掘技术，这一点对于普通的新闻记者而言绝非易事。[497]

除此之外，拉斯布里奇还有一个更为大胆的计划——寻求《纽约时报》的帮助，其实这一招他在针对维基解密的系列报道过程中就曾经用过。他拨通了艾布拉姆森的电话。2004年《纽约时报》的瑞森和利希特布劳打算发表他们揭露“星风”行动的重磅文章时，就曾经找到过艾布拉姆森，当时她是报社的副总编辑，后来接替名声不佳的凯勒成为报社总编。

对于跟《卫报》合作报道斯诺登文件的事情，艾布拉姆森非常重视，但电话里显然不适合谈论如此秘密之事的具体细节。为了合作成功，她和副总编辑悄悄飞抵伦敦，造访了《卫报》总部。在一张纸上，拉斯布里奇列出了10多个条件，临近结束，他还对艾布拉姆森说：“斯诺登和格林沃德对你们《纽约时报》可不太感冒，《卫报》的记者将加入你们的报道团队，和《纽约时报》并肩作战。”听到这话，艾布拉姆森苦笑了一下。[497]前段时间，《卫报》和大西洋彼岸的《华盛顿邮报》并肩战斗，掀起一波又一波新闻热潮，手上没有一手材料只能炒冷饭的《纽约时报》好生嫉妒，硬生生地把《卫报》挤兑成了一家“英国新闻网站”，把格林沃德贬损为一个“博主”。[368]不过，此时此刻，这些都变成了不值得一提的小事。艾布拉姆森很痛快地答应了拉斯布里奇开出的所有条件，两个竞争对手从此在斯诺登文件的刊载上展开了密切的

合作。

有了这些预防措施，拉斯布里奇心里总算放下了一块石头。他潇洒地把报社的大小事务统统交给副总编保罗·约翰逊（Paul Johnson），自己则去参加在法国举办的一个“钢琴夏令营”。[497]说起来，拉斯布里奇在音乐方面颇有造诣。他从小练习钢琴和单簧管，在英国国家青年管弦乐团当过好几年乐手。[407]在一本回忆录里，拉斯布里奇提到，自己即使在报社推进维基解密的报道工作那段非常繁忙的时间里，仍在学习演奏肖邦最难弹奏的一首作品——《第一叙事曲》。[497]他曾经跟夫人谈过，等到将来某一天离开《卫报》，他会去做一些与音乐有关的事情。[407]

总编走了，英国副国家安全顾问奥利弗·罗宾斯（Oliver Robbins）却又来了。最终，留守报社的副总编约翰逊和他达成一项协议：政府不再没收报社那些处理过斯诺登文件的计算机，由报社自己在政通局的“指导”下砸毁它们。接下来就发生了7月20日《卫报》总部地下室里那滑稽的一幕。

那么，触痛英国政府，促使他们进行“示范性销毁”的那一组文章到底说了些什么呢？

黄金时代

在介绍这些文章的内容之前，先要说说“时代”计划这个名字。中国国内多数人把它译作“颞颥”，的确，这是英文单词“TEMPORA”的意思之一，但这个词实在显得晦涩生僻。有理由怀疑这个单词用在这里，可能并非取它的英文意思，而是取它的拉丁语含义，意为“时代”。这种看法和《纽约时报》中文版基本一致，在一篇报道里，他们把“TEMPORA”翻译为“时光”。[504]

美联社在2005年曾有过一篇报道，美国海军把“吉米·卡特”号潜艇改装之后用于监听海底光纤电缆。想要监听光缆，最好是找到中继点，光缆在这些中继点的位置上不再是一捆，而是一根一根的，更便于搭线监听。[505]据称，美国有4艘潜艇专门从事海底搭线工作。由于光缆的粗细和25美分硬币的直径差不多，因而对它们进行操作若稍有不慎，就会对光缆造成损害，而这马上就会被运营商发现。[506]简而言之，水下作业并非易事，好在这样做也并非必须。光缆总要上岸，在它们的登陆站点上搭线，相对而言要方便得多。

从地理位置上讲，英国其实是一个非常理想的进行搭线监听的地方。在互联网世界里，英国的重要意义被很多人忽略——从北美大陆到欧洲，跨大西洋的海底电缆有很多都经过英国。[505]主干光缆大多在康沃尔郡的比德镇登陆。[507]大家可千万不要小瞧了这个比德镇，政通局很早就在这里建立了一个监听站，当时它的名字是“政通局莫文斯道站”，是“梯队”计划建立的第一个地面跟踪站，代号“大瓶”（CARBOY），主要负责侦听大西洋和印度洋上空的卫星通信。现在，这个监听站已经更名为“政通局比德站”，并且增加了一项新任务：对在比德镇附近海滩上登陆的跨洋光缆进行监听。[508]

只要英国政府批准、光缆的运营商同意，情报单位就可以进入他们的光缆登陆站点，安装一个很小的设备，在光缆信号不断流的情况下，把所有信号都复制出来一份，实现监听。严格说起来，信号并没有被“复制”，而是通过一个棱镜把信号分成两份，主要的那一份向着预定目的地继续流下去，而另外一份则流进情报单位。[505]这种做法在前文曾经提过，美国电话电报公司旧金山分部专门开辟出一个秘密小屋，主要就

是为了方便国安局做搭线分流监听这类事情。

和美国的“上游”计划类似，英国的“时代”计划也是跟其国内顶级的通信服务商“合作”，当然有时候这种合作这些公司并非心甘情愿，但通信服务商没有选择，政府部门拿出法律武器的时候，他们毫无还手之力——这两件武器就是2000年颁布的《调查权监管法案》（RIPA）和1994年颁布的《情报工作法案》（ISA）。手里有了这些武器，政通局就可以在服务商的电缆上搭线监听，拉网式地获取非英国人传输的通信数据。和“上游”计划一样，“时代”计划的工作模式也被称为“被动式搜集”，政通局可以守株待兔一般静等数据送上门。对通信服务商而言，他们必须参加，即使不愿意也必须参加，并且只能做、不能说。[509]

和美国国安局的“布拉尼镇”和“锦绣镇”等“上游”计划类似，到底哪些通信服务商参与了“时代”计划，这是政通局的重要秘密。他们反复告诫自己的员工，对于可能泄露公司底细的各种信息要小心处理。在内部，他们把这些通信服务商叫作“特殊情报源提供商”，又亲切称其为“监听伙伴”。[510]政府了解到《卫报》手里掌握了这些伙伴的很多情况，于是明确要求报社不要向外界披露这些情况。《卫报》方面考虑再三，为稳妥起见，听从了政府的意见。最终，有关情况还是由德国的《南德意志报》率先曝光出来，《卫报》这时才跟进报道，也免去了更多的麻烦。[511]

根据他们的报道，英国电信、沃达丰和威瑞森公司这三家大公司，以及环球跨越、第三层、通泰和互通四家相对小一点儿的公司都参加了“时代”计划，秘密向政通局开放了他们的海底电缆。政通局给这几家公司分配的代号，有的还勉强说得过去，比如英国电信公司代号“大法宝”（REMEDY）、第三层公司代号“小可爱”（LITTLE），而给通泰公司的代号为“玻璃体”（VITREOUS），这就有点儿不着调了，剩下的就有点儿恶作剧的意思了，比如威瑞森公司的代号是“的确良”（DACRON），而沃达丰公司的代号是“衰老期”（GERONTIC）。[512]

在这些合作伙伴当中，政通局和英国电信公司的关系最为密切，每次需要监听某个新的国际光缆的时候，他们通常会把这家公司的工程师找来，一起商量在哪些地方搭线安放传感器最为合适。[507]根据《华盛顿邮报》掌握的材料，除了政通局，世纪跨越还和国安局签有协议，在美国本土建立了一处秘密设施，官方把它称为“网络行动中心”。政府

人员提前30分钟通知公司之后，就可以进入这个地方，拿着具体的监视要求，监督公司雇员完成任务，究竟得到了哪些数据，即便是公司的高层也不允许知道。2011年，第三层公司从一家新加坡公司手里买下了世纪跨越的大部分股权。[506]

当然，政通局的监听行动并非总会征求光缆运营商的同意。“环球光纤链路”（FLAG）是经印度洋、连接英国和日本的一个国际光缆系统，链路中有两根光缆在比德镇登陆，一根编号为“大西洋1号”、另一根编号为“欧洲亚洲”，这两根光缆都被监听了，这是政通局在完全背着光缆主人的情况下做的一件事情。[507, 513]在比德镇附近的海滩上登陆的还有一根属于德国电信公司的“TAT-14”光缆，它也被政通局偷偷地监听了[508]。除了这些，有据可查处于政通局监听之下的还有“东南亚–中东–西欧3号”和“东南亚–中东–西欧4号”光缆，以及“大西洋跨越1号”“泛欧跨越”等10多根国际光缆。[513]这就是所谓的“要从此处过，留下数据来”。

这些光缆上岸之后，都要从英国的通信公司修建的登陆站里经过。所以，即便政通局不跟这些光缆的主人打招呼，也不用获得光缆运营商的同意，他们也必须跟英国这些通信公司合作。[512]例如，沃达丰下属的有线无线公司就把自己的登陆站提供给政通局使用，代号“黑种草”（NIGELLA）。[514]对于政通局在自己的登陆站里做的这些隐秘之事，合作伙伴们当然不能说、也不愿意说。

有了合作伙伴的支持，政通局可以掌控的光缆达到了1500～1600根，他们的目标是同时收割其中400根光缆上的数据。截至2012年，这个目标已经完成了一半。按照每根电缆每秒10吉比特的流量计算，政通局在理论上每天拿到的数据多达21.6拍字节（PB）。这么多数据，大致跟谷歌公司前几年每天从互联网上收割的数据规模差不多。过滤掉一些无用数据之后，内容数据可以保留三天，元数据可以保留30天。[510, 512]在某些场合，他们的这项工作被称作“特殊情报源开发”，而这项工作的直接成果又被称为“互联网缓冲区”。[515]正因为他们拥有的这种能力，《卫报》说政通局是情报世界里的一支超级力量。[516]

“时代”计划最初的起源，是政通局在康沃尔郡的比德监听站开展的一个试验性项目。这个项目进行了三年，到2010年，国安局的分析人员才开始接触通过这个项目搜集到的数据。[515]2011年夏，国安局人员进入比德监听站开展工作，同年秋，“时代”计划正式运行。2012年5

月，两家单位共有550名分析人员在这些数据上开展工作，其中有300人来自政通局、250人来自国安局。[516]

在2011年的一份报告上，国安局对政通局取得的成绩赞许有加，“政通局在元数据搜集方面已经超过了我们”[515]。政通局的领导并没有沉醉在搭档的表扬里而迷失方向，他们保持着清醒的头脑。在2012年的一张幻灯片里，负责“时代”计划的局领导提醒他的团队，新的技术使得政通局可以在光缆上看到大量的“光”，也就是各种新数据，过去5年他们看到“光”的能力提高了7000%，而分析和处理“光”的能力只提高了3000%。他说：

政通局正在开辟新的领地，测试我们的系统、处理所有的“光”。我们今天面对的挑战就是：从昨天的能力出发夺取明天的胜利。[517]

国安局和政通局之间的合作对双方都有好处。相比国安局，政通局需要面对的监管体系要宽松许多。[509]即便如此，政通局想对本国人进行监视还是要比对外国人监视麻烦一些。《连线》杂志据此推测，两家单位合作之后，双方可以分别绕开各自对本国人监视所必需的条条框框的限制：国安局监视英国人不受英国法律的约束，同样，政通局监视美国人也不受美国法律的约束。[518]

《连线》杂志的这种推测并非空穴来风，政通局在内部的一份报告里承认：“我们不像国安局，有那么多困扰他们的法律约束问题。在处理双方行动所面临的法律约束问题方面，我们乐见其成。”在他们的发展战略里，政通局描绘了三年后与国安局合作要达成的目标状态，他们说：“我们将充分利用我们独特的卖点，我们的地理位置、（我们和通信服务商的）伙伴关系、英国的法律制度以及技术熟练的人才队伍。”正是由于英国法律制度的这种设计，政通局才得以如此大规模地、不间断地从过境英国的互联网光缆上拿到数据。[517]

和他们的搭档相似，政通局也发展了自己的下线。比如在中东，他们就建有一个秘密的互联网监视站。按照调查记者坎贝尔的说法，有关中东监视站这件事情的密级非常高，被政通局列为第三级绝密。要知道，“时代”计划的具体情况只被列为第一级绝密，而参与“时代”计划的合作伙伴的身份属于第二级绝密，这些都要比中东监视站的密级低一些。位于阿曼锡卜的这个监视站是政通局“回路”（CIRCUIT）计划的一个组成部分，代号“吉他”（GUITAR），主要负责对经过霍尔木兹海峡

进入波斯湾的海底电缆进行监听，也被政通局称作“海外情报处理一号中心”（OPC-1）。在阿曼，除了这个监视站，政通局另外还有两个站点，代号“定音鼓”和“单簧管”，分别承担对伊拉克和也门的通信进行监听的任务。[507]

2010年，政通局在内部发布了一份报告，首先描述了一个巨大的互联网世界，全球有20亿网民，移动互联网的流量在一年内增长了600%。然后，报告话锋一转，写道：“不过，我们开始‘掌握’互联网了，并且我们现在的能力相当可观……我们现在进入了黄金时代。”[515]

“肌肉男”

斯诺登在接受采访时曾说，政通局比国安局还要糟糕，因为他们代表着首个“一网打尽”的系统。至于如何逃离“时代”计划，他的意见是：

如果可以选择，你就不应该通过英国的线路或者利用英国的服务器发送消息。只要有的话，即使是女王陛下和她保镖的自拍也会被记录下来……[505]

谷歌和雅虎公司恐怕没有想到斯诺登的这段话就是说给他们听的。在他们连接数据中心的光缆中，有一部分就在英国。2013年10月30日，《华盛顿邮报》刊登了戈尔曼等人撰写的文章，揭露国安局和政通局联手侵入谷歌公司和雅虎公司租用的英国电缆，这个合作计划代号为“肌肉男”（MUSCULAR），是国安局与盟友们合作开展的“防风布”计划的一个重要组成部分。

“棱镜”计划中，国安局借助法律手段，在公司的前门“理直气壮地”索要数据。那些公司尽管大多不太愿意，雅虎公司甚至拼命抵抗了一段时间，最终都不得不低头配合着做了不少事情，他们以为国安局应该心满意足了。没想到，国安局竟然贪得无厌，在其英国搭档那里找到了公司的后门，通过“肌肉男”计划，溜门撬锁，大量窃取数据。

面对媒体的追问，国安局表示：“肌肉男”计划只是针对国外情报目标的一个计划而已，他们采用的程序经过了司法部部长批准，也考虑了美国人的隐私保护问题，并且尽最大可能避免美国人的信息被“锁定、搜集、处理、开发、保存和散播”。可是，在“肌肉男”计划的文件里，国安局却是另外一副模样。对于谷歌和雅虎私用的那些网络上的数据，他们要“一网打尽”，“成批地、巨量地”获取。[491]国安局如此言行不一，怎能不让这些公司气愤。

政通局在“肌肉男”计划中的做法和他们在“时代”计划中的做法类似，他们把抓取到的所有数据都存进一个“缓冲区”里，数据会在那里保留3~5天。然后国安局开发的工具就派上了用场，对谷歌和雅虎公司使用特殊格式保存的数据进行解码，再根据预先设定的条件，把需要的数据挑选出来，把不需要的数据丢弃。[491]国安局和政通局做的这项“解

码”工作，在业界还有一个响亮的名字，叫作“反向工程”。

需要说明的是，“肌肉男”计划不属于《外国情报监视法案》及其修正案的管辖范围，它是通过第12333号总统令来获得授权的。对于这个总统令授权的各项情报活动，国会几乎从没有监管过。这一点就连参议院情报委员会主席菲因斯坦都承认了。[491]

有人告诉《纽约时报》，连接谷歌公司数据中心的光缆是由第三层公司负责运营的。也就是说，配合政通局和国安局窃取公司私有数据的就是这家公司。对此，公司方面当然需要站出来做一番解释，他们说：

公司要遵循业务运营所在国的法律。一般说来，在执法和安全调查等方面寻求帮助的那些政府，禁止公司披露有关这些帮助的信息。[519]

在斯诺登提供的有关“肌肉男”的幻灯片上，直接点出了谷歌公司的名字，并且，这张片子附带的注释上写道：国安局破解的是他们的电子邮件（也就是Gmail）的数据。相比之下，在“肌肉男”计划里，雅虎公司的损失可能更为惨重。

国安局的技术人员发现，雅虎公司在不同的数据中心之间传递邮件的时候，使用了一种叫作“Narchive”的数据格式。对雅虎邮箱的某个用户而言，他的账户总是属于雅虎的某个数据中心。一旦邮件系统发现把这个用户的账户搬到另一个中心读取速度会更快，系统就会使用Narchive格式，把他账户下的所有邮件打成一个数据包，转移到那个更快的数据中心里去。在转移的途中，这个数据包必然会经过一些光缆，到时就会被等候在那里的国安局截获。[520]

就在谷歌和雅虎发现自己的数据中心被国安局和政通局联手入侵的时候，微软公司在一边看热闹。不过，微软公司心里并不踏实。没过几天，一直积极、主动、愉快地与国安局合作的微软公司发现，自己很可能并没有逃脱“肌肉男”计划的魔掌。证据虽然并不是那么确凿，但看到自己的电子邮件系统和在线聊天系统也在国安局的幻灯片里被点了名，而自己提供的一种网络认证服务也出现在国安局有关“肌肉男”计划的一封电子邮件里，公司心里应该已经明白了大半，更明白自己不可能去找国安局对质，只能是哑巴吃黄连——有苦说不出了。[521]

谷歌公司的总信息官发表声明说：“政府部门竟然这样从我们的私有

光纤网络上截取数据，我们非常气愤。”作为官方声明，这是公司方面最强硬的一种表态了。私下里，谷歌公司的员工可就不需要这么克制了。他们在自己的博客上大爆粗口、发泄愤怒。其中，谷歌公司的一位安全工程师是这样写的：

我不是美国人，我是英国人，但这没什么区别——政通局原来比国安局更糟糕……（好在）这些幻灯片里的数据流现在都加密了，国安局和政通局的那些家伙为了获取这些数据所做的一切都没用了。[522]

其实，谷歌公司早在一年前就着手处理数据中心之间的通信安全问题了，按照这位安全工程师的说法，在“肌肉男”计划曝光之时，公司已经采用了更加强大的加密措施来保护数据中心之间的通信安全。公司总裁埃里克·施密特就说过：“要应对政府部门的监视行动，解决方案就是把所有的东西都加密。”[523]

雅虎公司则慢了整整一拍，其首席执行官玛丽莎·梅耶（Marissa Mayer）承诺：公司将在2014年3月底对数据中心之间传递的所有信息进行加密。还好，她的这一承诺按期兑现、没有失约。[524]同样滞后的还有微软公司。他们连夜开会，赶紧宣布公司制订了工作计划，对数据中心之间的通信进行加密，以对抗政通局和国安局的监视行动。微软公司的数据安全策略更为彻底，加密不仅针对数据中心之间的通信，在同一个数据中心内部，服务器之间的数据传输也都被加密了。[525]

经过了这么一番折腾，几家公司的心中都留下了阴影，再也不会认为自己的数据安全可以高枕无忧，因为政通局和国安局随时有可能再次找到他们的某个漏洞，把受到层层保护的数据窃取出去。这就叫“不怕贼偷，就怕贼惦记”。

政通局的“能力”这么强，公众一片哗然。于是就有“知情人”站出来讲话，试图缓和一下紧张的气氛。他说，政通局收集的数据就像一个“巨大的草堆”，这给普通人留下一种错误印象，以为政通局会阅读成千上万封电子邮件，其实他们根本没有，为了从数据的“草堆里把几根针挑出来”，政通局不需要检查每根稻草。具体地说，他们有一种办法，可以直接抛弃或者跳过大量的数据，只把那些针留下来。[516]

《斯诺登档案》的作者卢克·哈丁（Luke Harding）说，“草堆”是政通局局长伊恩·洛班（Iain Lobban）最为钟爱的一个比喻。其实英美情报

圈里的很多人都喜欢用这个比喻，实在不知道上面提到的这位“知情人”是不是洛班局长。斯诺登很不喜欢这个比喻，他说：

我认为，简单地使用“草堆”这个词就是误导公众。它的背后其实是一大堆人。“草堆”里满是最为私密的个人记录，它们被集中在一起，一遍一遍地被整理，越来越频繁地被保存。监视我们去的每个地方、做的每件事情，分析我们说的每个词，评价我们的每次联系、爱过的每个人，通过这些手段来发现恐怖密谋或者犯罪企图，难道这就是我们所希望去生活的社会吗？[526]

“五只眼”

政通局把从光缆上搜集到的大量数据共享给国安局，还把监视基地拿出来跟他们的战友共享。国安局当然不能白占便宜。据《卫报》透露，在自2011年以来的三年时间里，国安局至少向政通局支付了1亿英镑的费用。为了对得起这些钱，政通局必须很努力才行，于是他们在战略文件里写道：我们必须尽心尽力，并且要让国安局看到这一点。[527]

说起来，20世纪60年代，政通局建设莫文斯道监视站的大部分经费还是由国安局提供的。所以监视站一竣工，当时的政通局局长伦纳德·胡珀（Leonard Hooper）就致电国安局局长马歇尔·卡特（Marshall Carter），表达他个人的谢意。胡珀建议：比德这个监视站的两座天线应该命名为“帕特”和“路易斯”！[114]“帕特”是卡特局长的绰号，“路易斯”则是托德拉副局长的名字。胡珀局长的建议颇有些溜须拍马的意味。不知道莫文斯道那两座巨大的天线最后是不是真的这样命名了。

在《秘密机构》一书里，班福德说，英国政府一直担心国安局某一天会离政通局而去。他们的这种担心，在马岛战争期间达到顶点。国安局破解了阿根廷方面的通信密码，英国截获的阿根廷军事情报中有98%来自国安局。直到这个时候，英国政府才深切地感受到，他们在信号情报方面已经完全离不开国安局的帮助了。[528]当然，再精明的猴子也有掉下树的时候。国安局也曾遭遇马失前蹄的尴尬。前面曾经讲过，2000年1月国安局发生过一次严重的“系统错误”。在陷入“昏迷”的三天多时间里，原本应该由国安局监视的通信流量转给了政通局。事后，政通局的一位官员就说：“我们把所有事情都担了下来”。[114]

更多的尴尬还是留给了政通局——历史上英国的信号情报力量曾经远远强于美国。

现代信号情报的历史发轫于第一次世界大战。战后，英美两国信号情报单位的命运却完全不同。1919年11月，英国人把各种信号情报人员聚拢起来，成立了一个高度秘密的单位，对外的名义是“政府密码学校”。它的定位非常明确：英国密码研制和破译的中坚力量。并且，这个名称也并非完全是幌子。当时顶尖的密码破译人员要用很多时间给新来

的生手讲授课程。[529]相比之下，美国人的信号情报单位“黑室”的运气就没有那么好了。1929年，美国国务卿发现隶属于国务院的这家单位不仅在破译敌国密码，并且在自己眼皮底下破译盟国密码，随后便怒不可遏，下令黑室立刻关门歇业。几个月后，陆军在机关里面悄悄成立了一个单位，叫作“信号情报处”，工作场所被安排在一间非常狭小的库房里，更加秘而不宣，既要防止敌人知道，还要防止外交部门知道。虽说带有“恢复”性质，但骨干已经大量流失，新单位的力量非常弱小——只有一个工作人员，他的名字叫威廉·弗莱德曼（William Friedman）。[530]

随着“二战”临近，政府密码学校不声不响地从伦敦搬到了布莱奇利庄园，还启用了一个新的通信地址：布莱奇利市第101号信箱，时间是1939年8月。几周后，英国对德宣战。[531]这个庄园距离伦敦只有47英里（大约76公里），正好位于牛津大学和剑桥大学之间，这样一种安排方便情报单位从这两所世界顶尖的大学里招聘新的工作人员[490]，而“政府密码学校”这个掩护名称也会让外人以为这里只是由几个学校组成的一个“大学城”。

英美情报单位曾经在第一次世界大战期间合作过，不过那并非一段愉快的经历，而是充满了怀疑、焦虑甚至不信任。这次再度走到一起，对双方能开展什么样的合作、合作深度如何，没人有把握。美国黑室解散之时，正碰上美国股市大崩盘。原先领导黑室工作的赫伯特·亚德里（Herbert Yardley）发现自己除了写作，别无他途，于是笔耕不辍，两年后便出版了一本饱受争议的著作，书名就叫“美国黑室”。他在这本书里把自己的秘密工作经历和盘托出，英国人认为他说了很多不该说的话，等到听说亚德里跑到加拿大情报单位干活，就警告加拿大人说，只有先把亚德里开除，才会接纳加拿大人进入大不列颠信号情报俱乐部。面对人少体弱的美国情报同行，英国情报单位更为冷淡，与之交往更加谨慎，有了亚德里这样一个先例，美国人在他们眼里，多半都不太可靠。[532]

相比之下，美国人则慷慨得多。他们把最新破译的日本“魔术”密码以及仿制的密码机全共享给了英国同行。事后证明，英国人自己也不太谨慎：美国人仿制的日本密码机刚被运到新加坡，那里就沦陷了，密码机至今下落不明。[532]

英国人最初设想的与美国人之间的合作颇有几分“各人自扫门前

雪”的意思。他们认为，美国人应该集中精力解决日本的密码问题，而德国的“恩尼格码”问题则应该交给英国人来解决。他们在1941年就告诉美国人“恩尼格码”的一些情况，但对于处理德国密码的具体做法，英国人则留了一手。简单来说，英国人不希望他们的美国搭档也去研究德国密码。但这只是英国人一厢情愿的想法，因为美国人已经在跨越大西洋的途中和德国人遭遇过了，他们也需要破译德国的“恩尼格码”。[532]

“恩尼格码”这个名字源于希腊文，意思是“谜”。大约在20世纪20年代，德国军方开始放弃原来用手工方式生成密码的做法，改用一种商业化的密码技术，这就是“恩格尼玛”。这项技术在当时已经广泛地应用于银行和商务，可以产生非常难以破译的密码。德军的“恩尼格码”让盟军非常头痛，在解决这样一个难题的过程中，大西洋两岸涌现了一批耀眼的科学明星，其中就有一位名叫图灵的年轻人。后来，为了纪念这位计算机科学天才，计算机界的最高奖项就被命名为“图灵奖”。为了破译德国人的“恩格尼码”，图灵设计出了一种机器，被称为“炸弹机”。有了这些“炸弹机”的帮助，英国人开始源源不断地把德国人的密电破译出来。

但是，英国人最担心的事情还是发生了：德国海军改进了他们的密码机器，使其具有更好的加密效果，这意味着需要更多的“炸弹机”破译新的密电。而此时英国人却遇到了一个大麻烦：他们的生产能力不足，无法生产足够多的“炸弹机”。大概就在这个时候，美国人追了上来。1942年9月，负责美国海军密码工作的约瑟夫·温格（Joseph Wenger）提出，要投入200万美元购置230台“炸弹机”。这实在让英国人眼红，因为布莱奇利庄园能得到的“炸弹机”只有20多台。英国的密码专家意识到，他们的美国搭档将要以一种工业化的规模破译敌方的“恩尼格码”，他们在这个方面的领先地位一去不复返了。[532]当然，身处困境的英国人也认识到，此刻他们非常需要美国人的帮助，必须紧紧地和美国人捆绑在一起。

也就在1942年9月，英美信号情报部门缔结了第一份协议，史称“霍顿协议”。准确地说，签署这份协议的，一边是政府密码学校的海军情报部，另一边是他们的美国海军盟友，针对的主要是德国海军。让英国人想不通的是，关于这份协议，美国海军没有向他们的陆军战友透露过一个字。1943年5月，英美两国签署了另一份协议，这就是“不列颠与美国通信情报协议”，英美开始在德国陆军和空军情报方面寻求合作。这个合作协议是英国人分别跟美国海军和陆军签署的，之所以出现这样一种奇

怪的现象，是由美国当时的军事管理体制决定的，对美军各军兵种进行集中管理的美国国防部那时候还没有建立，空军也还没有从陆军独立出来，这也就造成海军和陆军的情报部门自说自唱、各行其是。[532]

英美两国的情报同盟关系并没有随着“二战”的结束而终止。大战结束之后，美国总统杜鲁门对美国的情报工作可谓有破有立。一方面，他关闭了战略工作办公室，直到几年后，中情局才在这个单位的废墟上重新建立起来；另一方面，他十分重视信号情报的价值，积极巩固与英国之间的信号情报同盟关系。1946年3月，英美两国的代表秘密签署了“联合王国与美国协定”。伦敦信号情报委员会的帕特里克·马尔约翰逊（Patrick Marr-Johnson）上校代表英方，美方的代表则是国务院与陆海军通信情报委员会的霍伊特·范登堡（Hoyt Vandenberg）中将。兄弟俩商量好交换各自监听、破译和翻译的国外通信情报，他们在协议中写道：“任何向第三方透露本协议存在的行为都将被视为违反了协议。”[533]如果协议一方要与第三方联合行动，它必须获得协议另一方的同意，在此之前它不能采取任何行动。[534]协议规定：

这样的（情报）交换将涵盖所有将开展的（情报）工作，不设限制，仅当一方要求并经另一方同意后才会排除在交换范围之外。双方都愿意将这样的例外降至最少，并对报告的且双方同意交换的情报不设限制。[534]

这种协议背后是双方的高度互信。起初，参加这个协议的成员并不包括其他英联邦国家，因为这些国家都由英国人全权代表了。在协议签订之前，政通局组织召开的信号情报工作会议刚刚结束，加拿大、澳大利亚和新西兰信号情报单位派代表参加了会议。这次会议被看作英国人为了与美国人签协议，提前做的一项准备工作。[535]

澳大利亚仿照英国模式，建立了一个类似于政通局的单位，对外称作“国防安全处”（DSB）。关于处长人选，澳大利亚方面推荐了四个人，都是富有作战经验的军事情报官员。不过政通局告诉他们，处长必须是英国人。事情后来还真就这么办了。国防安全处的首任处长就是英国人。直到20世纪50年代，这个位置才由澳大利亚人接任。[535]

两年后的1948年，加拿大决定正式加入情报交换同盟，不再由英国人代表自己。于是同盟有了三个成员。新的协议文件指出：

无论平时还是战时，信号情报的重要性无论如何强调都不为过，必须教导接触信号情报的那些人，这些情报极为敏感，必须加以保护。而熟悉信号情报搜集方法的工作人员应该成为重点保护对象，不能让他们执行涉险的任务，以免他们被敌人或者第三方抓获。[533]

又过了8年，澳大利亚和新西兰也加入进来，5个英语国家共享和交换信号情报的联盟终于形成。在他们共享的情报资料上大多都明显地标识出“USA, AUS, CAN, GBR, NZL”字样，或者是“AUS/CAN/NZ/UK/US EYES ONLY”字样，经常也会简单地标成“FVEY”，久而久之，情报圈中对该联盟就有了“五只眼”这么一个诨号。[536]

“梯队”

“五只眼”联盟的监听站能够覆盖全球绝大部分地区，于是就有了以监听全球卫星通信为目标的“梯队”行动。时至今日，对于它的存在，美国政府仍断然否认，英国政府则含糊其辞。[537]

1964年国际通信卫星组织成立，这个组织计划利用全球通信卫星，提供长途通信和洲际通信线路。他们的卫星刚刚上天，“五只眼”情报单位就已经悄悄行动起来，策划如何侦听这些卫星传送的信息。[538]

要截取通信卫星上的信息，首选策略是建立地面跟踪站。1971年，首个跟踪站在英国康沃尔郡的莫文斯道开始投入使用，代号“大瓶”（CARBOY），主要负责侦听大西洋和印度洋的卫星通信。接着投入使用的是美国西雅图的亚基马跟踪站，代号“杰克刀”（JACKKNIFE），主要负责侦听太平洋上空的卫星通信。最初，这两个跟踪站完全能够胜任监听所有国际通信卫星的工作，但由于卫星通信发展很快，“大瓶”和“杰克刀”难以应付，更多的跟踪站被建立起来。“五只眼”中的另外三只眼，加拿大、澳大利亚和新西兰在20世纪80年代中期加入了“梯队”计划。此外，挪威、丹麦、德国和土耳其等国后来也与美国和英国签订了信号情报共享协议，但它们的地位低于“五只眼”，被称为“第三方”国家。

除了建立更多的地面站，一批通信情报卫星也被发射升空。这些卫星或是悬在某些选定的地面目标上方，或是“陪伴”在其他卫星的身边。无论是哪一种，它们的主要任务都是密切监听目标发出或者接收的通信信号。比较著名的通信情报卫星有“峡谷”（CANYON）及其后继的“漩涡”（VORTEX）、“流纹岩”（RHYOLITE）和“大酒瓶”（MAGNUM）等。

因而，地面站可能同时具备多种监听功能，一是直接监听对方的通信卫星，二是接收己方通信情报卫星监听到的地面目标和空间目标信号。例如，英国曼威斯山地面站就身兼多职，在“梯队”计划里，它的代号是“月亮便士”（MOONPENNY），除了监视卫星，还要分别利用“跑道”（RUNWAY）系统和“绣线菊”（STEEPLEBUSH）系统操控“漩涡”卫

星和“大酒瓶”卫星开展侦听工作，[539]所有侦听到的信号都会交给“丝绸值”（SILKWORTH）系统处理。[538]

关于“梯队”计划的内容和范围，有多种认识。有人认为这个计划无所不包，涵盖了对卫星、海底光缆、互联网等各种通信手段的监视，甚至有人把这个计划和“五只眼”联盟混为一谈。形成这些“错误”认识情有可原，毕竟所有这些说法都像是在做拼图游戏：根据非常少量的资料进行猜测，同时想把所有相关资料综合整理成一个整体。但随着美国情报机构的秘密资料逐渐曝光，特别是借助于斯诺登集中曝光的这批资料，“梯队”计划应该只是以美国为首的情报共享联盟开展的诸多工作中的一项，他们之间签署的情报共享协议应该是一种框架性的文件，原则性的内容多，具体操作层面的内容少。对于不同类型的情报源，很可能需要落实为不同的具体行动和计划，比如对于地面的无线电信息，就是“火车头”计划；对于卫星通信信息，就是“梯队”计划；对于互联网信息，则是“防风布”和“护城墙A”等计划。当然，参与每个计划的成员国数量可能不尽相同，但以美国为首的“五只眼”国家几乎总是核心成员。

除了整合地面站力量、共享地面站获取的数据，联盟成员还在各自的总部建立固定的联络办公室，互派联络官员。例如，美国国安局就在英国的政通局里设有专门的办公室，反过来，政通局在国安局总部也设有自己的办公室。有了这样一些机构，联盟的各项具体工作就一直运行得比较顺畅。美英两国在1981年建立起有史以来第一个全球数字广域网络，把信号情报站、卫星地面站和数据处理中心连接起来。这个情报网络规模之大，直到20世纪90年代中期才被国际互联网超过。[538]

1988年，福特航天公司和洛马公司前雇员玛格丽特·纽什（Margaret Newsham）向美国媒体披露了“梯队”计划的有关情况。纽什作为软件工程师为国安局工作了10年时间，其中就有两年是在曼威斯山地面站度过的。一天，她发现她参加的“梯队”计划不仅监视外国人，而且监视自己的同胞，哪怕国会议员也不能幸免。她检举了公司的贪腐和开支不当等情况，可没想到的是，公司毫发无损，她却惨遭解聘，然后等待她的是自己家庭破裂、身患癫痫、几乎瘫痪。英国记者坎贝尔专门对“梯队”计划进行了调查。他发现，在曼威斯山地面站工作的有1200多人，其中2/3来自美国，而不是来自英国本土。可惜他的文章《有人正在偷听》当时没有引起外界注意[539, 540]，直到若干年后，人们才发现了这篇文章的真正价值。

1996年，一本题为“秘密力量”[注]的书出版，“梯队”计划才开始被世人关注。为了写这本书，新西兰记者海格用了好几年的时间，其间还得到了新西兰情报单位许多工作人员的支持和帮助。他对胡帕跟踪站进行了深入调查。在“梯队”计划里，这个跟踪站的代号是“燧发枪”（FLINTLOCK），负责跟踪南太平洋上空的国际通信卫星。

欧洲议会在海格这本书内容的基础上，花费了几年时间开展调查，此时正值国安局的海顿局长上任，百废待兴。欧洲议会先后在2000年和2001年完成了两份报告，报告中写道：借助“梯队”计划，美国公司多次在与欧洲公司的竞争中“赢”得先机。1994年，沙特航空公司准备投资60亿美元更新机队，空中客车公司当然是全力以赴，进展也算顺利。但空中客车公司并没有想到，自己与沙特航空公司和沙特政府之间的传真和电话都被笼罩在一张恢恢天网之下——布下这张“天网”的就是美国国安局。国安局很快就发现，空中客车公司正在以钱铺路，贿赂沙特政府官员。抓住对手的这个“尾巴”后，美国政府立刻向沙特政府施压，最终，空中客车公司两手空空，胜利属于美国的麦克唐纳·道格拉斯公司。[541]同一年，德国西门子公司和阿联酋的一笔1.19亿美元的生意被美国电话电报公司抢走。[542]所有这些的背后黑手都是“梯队”计划。

对此，前中央情报总监伍尔西在《华尔街日报》上发表过一篇文章，题目就是“为什么我们要监视盟友”，字里行间颇有点儿“我是流氓，我怕谁”的味道。在这篇文章里，伍尔西毫不客气也毫无遮拦地写道：

没错，欧洲的朋友们，我们一直在监视你们，因为你们在行贿。与你们的美国对手相比，你们的产品或者价格昂贵，或者技术逊色，或者两者兼而有之。因此，你们花很多钱行贿。你们的政府同流合污，在某些欧洲国家，行贿甚至不用交税。我们揭露了你们的行径……我们去找被你们收买的政府，告诉他们，我们不喜欢这种腐败行为。他们通常就把全部或部分合同给那些报价最好的公司，有时是美国公司，有时不是。[115]

国安局其实并不否认自己在收集经济情报，但他们狡辩说自己并未把这些情报“直接”提供给美国公司，而是按照联邦政府的要求，以比较间接的方式为美国公司提供支持，一种途径是努力查明外国竞争对手是否使用贿赂等非法和欺骗性手段获得优势，另一种途径是在重要贸易谈判中，向美国政府谈判人员提供情报。[115]这就是他们给自己设定的“是非”标准。

“梯队”计划包含的计算机系统数量很多。1982年，洛马公司得到了国安局的一项任务，建设“梯队”地面站的自动数据处理设备标准工具包，其中罗列了完成“梯队”计划任务所需的若干子系统。考虑到执行这个任务的年代，这份清单显得非常“古老”，但还是值得看一看的。这个工具包里主要包含了这样一些东西：本地管理子系统、远程管理子系统、通信处理子系统、电报消息处理子系统、频分多路复用电报处理子系统、时分多路复用电报处理子系统、语音处理子系统和传真处理子系统。[543]

这些子系统基本上都属于比较外围的、基础性的系统。在所有的“梯队”地面站里，处于核心的是被称为“字典”的计算机系统，这一系统运行在若干台DEC VAX小型机上。从流程上看，“字典”系统位于前端搜集系统之后，通过预设一些关键词，自动地从大量侦听数据中把有关信息过滤出来。2000年前后，国安局开始大力研发更先进的“话题分析”技术，用来代替“字典”系统中基于关键词匹配的技术。[543]

就在斯诺登到日本工作的那一年，一部以“梯队”计划为背景的好莱坞电影登上银幕，片名就叫“梯队阴谋”。可惜在中国国内上映时片名变成了“夺命手机”，彻底切断了这部电影与“梯队”计划的关系。当然，电影本身对“梯队”计划的解读是草率且不准确的，情节也是好莱坞擅长的那个套路：小人物不知不觉卷入大阴谋，然后绝地反击取得成功。在这部电影里，大阴谋就是国安局以反恐为名建立的“梯队”系统，利用它可以操纵世界各地的公共摄像头，甚至能查阅世界上任何人的电话记录和手机短信。主人公被各路人马追杀，面对国安局布下的天罗地网，他准备逃向何方？莫斯科！不知道斯诺登当年是不是也看过这部惊悚电影——因为莫斯科正是他日后避难的地方。

2011年，在“五只眼”联盟的秘密会议上，国安局发布了新的搜集策略：全面嗅探、全面合作、全面开发、全面处理、全面搜集、全面知晓。这是一幅宏伟的蓝图。在全面合作部分，明确提出要与英国政通局加强合作、要通过三泽基地加强情报共享等。这幅蓝图贯彻了亚历山大局长长期以来坚持和宣扬的“全面搜集”的思想。

亚历山大局长在2008年夏访问曼威斯山地面站时，曾经半开玩笑半当真地说：“为什么我们不能一直全面搜集所有的信号情报呢？”[544]熟悉局长的人说，亚历山大的策略和谷歌是一样的，那就是“占有所有的数

据”。对于手中掌握的强大的技术力量，亚历山大和他的前任海顿局长在处理问题时明显不同。海顿的态度是：我们应该使用这些技术力量吗？亚历山大的态度则是：我们有这样的能力就应该使用它们。他认为，为了防止恐怖袭击，必须尽可能多地占有数据，不仅要掌握最新的通信数据，还要掌握历史数据，以便利用这些数据发现恐怖活动的演进规律。当然，他的这些想法很可能违反了美国法律，但他似乎把那些条条框框全都扔到了一边。所以，媒体把他称作“国安局牛仔”。[545]

澳方情报单位对“五只眼”联盟的协议严格保密，以至于澳大利亚政府方面有近20年的时间被蒙在鼓里。直到1973年的一次偶然事件，澳大利亚政府发现了这个协议，这才知道松峡监听站竟然是与美国人共同使用的。除此之外，情报部门的其他一些秘密也首次为政府所知。一怒之下，威兰姆总理让两个情报部门的负责人下岗。这是另外一段故事了，有兴趣的读者可以自行利用谷歌或者百度搜索。关于这位总理，还可以多说一句话，作为反对党领袖，他曾在1971年访问过中国，受到过周恩来总理的接见。

---

1. 该书英文原名为：Secret Power: New Zealand's Role in the International Spy Network，作者是Nicky Hager，由Potton & Button出版社于1996年出版。——编者注

“锆石”

1985年1月24日，美国的“发现”号航天飞机完成了一次特殊任务。该任务之所以特殊，是因为这次飞行是首次利用航天飞机来执行情报任务，它携带着一件特殊货物，一颗代号为“大酒瓶”的通信情报卫星。进入预定轨道后，卫星打开了它巨大的天线，就像一把大伞，样子甚是壮观。[546]这一切英国人都看在眼里，他们在羡慕之余也夹杂着丝丝酸楚。

和美国人不同，英国的信号情报工作一开始就实行了集中管理，避免了不同军种之间的竞争，但他们总是被另外一个问题困扰：经费不足。相比之下，美国人的投入则显得充足得多。20世纪70年代，国安局的“流纹岩”卫星上天之后，政通局就提出过发展情报卫星的建议，可是，这些建议不断被提出，不断被上面否决。[528]等到所有人都认识到信号情报的未来属于太空的时候，英国的政通局发现自己已经远远落在美国人的后面了。[546]

在马岛战争中，英国政通局不得不依赖美国国安局的卫星来获取情报，而要覆盖到作战区域，必须请求美国人不时移动一下这些卫星的位置。尽管两个兄弟间的关系很好，但美国人也只答应每天提供几个小时的服务，这还是政通局局长布莱恩·托维（Brian Tovey）争取了很多次才得到的。[546]1985～1988年担任国安局局长的威廉·奥多姆（William Odom）就说：

大不列颠为“二战”付出甚多，现在却不再付出了……如今，这项工作需要巨额投入，但是他们没有做到。[546]

他还说：

如果你们以为美国人还会免费给你们提供卫星系统服务，并且因此不把所有钱都投进去建设一个卫星系统，那将是十分愚蠢的。[546]

这些话深深刺痛了英国人。看别人脸色吃饭的滋味不好受。一直以来，美国人把使用它们情报的权利当作棍子，时不时拿出来敲打敲打他们的这帮哥们儿。爱德华·希思（Edward Heath）首相上台后执行“欧洲

优先”政策，这让美国总统尼克松和他的国家安全事务助理基辛格颇为不爽。基辛格决定给希思一点儿颜色瞧瞧，他对总统说：

> ……他们把所有情况都跟其他欧洲国家说了，事先不告诉我们，事后也不跟我们说。我要求他们跟我们保持通气，他们竟说，没有义务把他们欧洲人内部讨论的情况都告诉我们，可以（等事后）一次性地跟我们说。因此，我现在要切断他们从我们这里获取情报的途径。如果他们不把他们自身与整个欧洲的事情都与我们分享，我们就不把他们当作特殊的朋友。

情报部门告诉总统，双方交换情报是有言在先，几十年前签的协议一直有效。但“切断”的命令还是执行下去了。1973年8月，英国情报部门发现许多情报源突然被切断了，特别是来自卫星和飞机的图像情报。这让他们非常恐慌。[547]但希思首相就不只是恐慌了，他很生气。

仅仅两个月后，首相就等到了还以颜色的机会。10月，赎罪日战争注爆发，美国人想使用英国人在塞浦路斯的监听站和空军基地。这回轮到希思说“不”了。从此英美情报共享的合作推进陷入僵局，直到1974年尼克松总统因为“水门事件”下台之后双方合作才逐步恢复。[547]

曾经遭遇“切断”情报源的还不只英国。1990年伊拉克与科威特之间危机升级，海湾战争爆发，美国要求他们的北方邻居加拿大提供帮助，派军舰前往海湾助阵。加拿大军舰陈旧，舰上只有反潜装备，于是拒绝了美国人的要求。这下可把美国人激怒了，立刻切断了加拿大人的情报来源，让他们“统统黑屏”。压力之下，加拿大只得屈服。为了纪念这段难忘的历史，加拿大军方把这次出兵海湾称为“摩擦行动”。[547]

马岛战争之后，英国人启动了一个代号为“锆石”（ZIRCON）的卫星计划，撒切尔夫人甚至发出过“绷紧每根韧带，一定要让锆石上天”的豪言壮语。但是，英国人发现，研制和维护这样的卫星所需要的经费实在惊人，远远超出了他们的承受能力。[546]

到了1987年，他们开始盘算，是不是从美国人手里买一颗现成的卫星会更划算。但要做到全球覆盖，一颗卫星是不够的，至少需要三颗卫星。于是他们又想出了另外一种更为合理的解决方案：支付5亿英镑，租用美国人新一代的“大酒瓶”信号情报卫星系统。根据协议，政通局可以使用这些卫星1/3的工作时间搜集他们自己感兴趣的情报。[546]外交

大臣理查德·豪伊（Richard Howe）就说：

如果白吃白拿，就不能做到有所选择。既然不能完全独立地运行（卫星系统），那就应该花一些钱、分担一部分系统（运行的）费用。[546]

就在英国人自行研制的情报卫星所执行的“锆石”计划即将下马之际，长期跟踪研究政通局的调查记者坎贝尔却准备向英国广播公司曝光这个投入很多却最终夭折的项目。他惊奇地发现，对于这个开支如此庞大的计划，议院竟然一无所知。这番情形和若干年前的另一桩丑闻如出一辙。[546]

可是，有关他的这档节目要播出的风声提前被泄露出来，引起了政通局的高度关注，局长立刻找到广播公司进行协商。1987年1月，广播公司总经理宣布：出于国家安全方面的考虑，坎贝尔的那档节目被禁止播出。不仅如此，高等法院还发布了禁令，禁止坎贝尔播放他拍摄的纪录片，也不允许他发布其中的任何内容。第二天，倔强的坎贝尔就通过《新政治家》杂志把“锆石”计划这一丑闻捅了出来，他还试图在下议院播放他的影片。政府终于被他的这些做法惹恼了，下令查抄了英国广播公司和《新政治家》杂志社，当然，坎贝尔的家也不能幸免，一并被查抄。[546]

说起坎贝尔，多年来他一直是让英国政府头疼的人物。1976年之前，就连是否存在政通局这么一个单位，都是一个很大的秘密。应该说，这个秘密被保守得相当好。“二战”之后，为掩人耳目，英国所有单位名称都弃用了跟密码有关的字眼，政府密码学校也更名为“政府通信总局”，并且从布莱奇利庄园搬到了切尔滕纳姆，在那里新建了办公大楼。尽管各种信号情报行动一天也没有停止，可它几乎完全藏身在其他情报单位的阴影里，几乎没人知道它的存在。[528]提到英国情报单位，人们最熟悉的就是军情六处，因为“007”系列电影中的詹姆斯·邦德太深入人心了。在这一点上，大西洋两岸的情况非常相似，美国这一边曝光率最高的情报机构要数中情局，而最新、最强硬的情报特工形象大概要算杰森·伯恩（Jason Bourne）了。

1976年夏，坎贝尔与其美国同行马克·霍森鲍尔（Makr Hosenball）合写的一篇文章刊登出来，题为“窃听者”。文章不过两页，而且只是登在一份印量很少的小众杂志上，但还是引起了轰动。在这篇文章里，他

首次向世人披露了政通局的存在、它的主要任务、它与美国国安局的密切关系、它采用的种种最新监视技术等诸多秘密。《政通局全揭秘》注一书的作者理查德·奥德里奇（Richard Aldrich）评价说，他的这篇文章是“开创性的”。所谓“开创性”有两重含义，首先是因为坎贝尔把政通局存在这一事实率先揭露出来，其次他在写作时采用了一种方法：利用公开发表的各种材料，小心翼翼地把其中一些被人忽视的片段拼接成了一个整体。班福德后来就采用了他的这种方法，利用公开信息源进行研究，写出了《迷宫》（*Puzzle Palace*）一书，首次系统地向世人讲述了国安局的种种故事。[548]

政通局对坎贝尔他们的这篇文章非常恼怒，霍森鲍尔很快就被驱逐出境，坎贝尔则被密切监视。就在这时，一个名叫约翰·贝里（John Berry）的信号情报兵找到了坎贝尔和另外一名记者克里斯平·奥布里（Crispin Aubrey），向他们诉说自己的战争经历。1977年2月，三人同时被捕并以触犯英国《保密法》被起诉。因为三个人姓氏的首字母分别是A、B和C，这桩案子便被人们称为“ABC审判”。[548]

出乎政府意料的是，随着审判的进行，政通局的内部情况越来越多地为更多人所知，比如他们在塞浦路斯的行动，原本并没有被坎贝尔曝光的一些事情也被捅了出来，完全违背了他们最初抓捕坎贝尔的初衷。更让政府难堪的是，这几位嫌犯发布的所谓秘密信息，竟然都出自类似于《皇家信号团》杂志这类的公开资料。只不过那些躲藏在犄角旮旯里的只言片语被坎贝尔等人细心地收集、串联起来，最终形成了他们的文章。[548]

这样一种情形，就连原本支持对三人进行起诉的英国外交大臣都看不下去了，强烈要求放弃该案。最终，对坎贝尔等人的绝大多数指控被撤销，案件以三人承认轻微违反《保密法》而草草收场。[548]

“ABC审判”是政通局历史上的一个标志性事件。从此以后，在世人眼里，政通局就被看作英国信号情报中心，尽管事后官方仍然拒绝承认，但有关它的前身政府密码学校、它在情报界中的地位、它下属的一些监视站的情况以及它与美国国安局的关系等，已经被无数的媒体传播开来。

---

1. 赎罪日战争，即第四次中东战争，发生于1973年10月6日至10月26日。——编者注
2. 书名原文为：GCHQ: the Uncensored Story of Britain's Most Secret Intelligence

Agency，由哈珀柯林斯出版集团于2010年6月出版。——编者注

豪夺与巧取

除了需要更多的经费，政通局还需要从数据“草堆”中挑出针来的工具。国安局一如既往，“慷慨”地把他们研制出来的工具提供给了政通局。最重要的一种工具叫作“X关键分”。

国安局和政通局建立了许多搜集数据的监视站，有些站点直接在通信光缆上搭线搜集。从技术上讲，不可能把搜集到的所有数据都传回国安局和政通局的数据中心进行处理，因为这需要铺设有同样数据容量的光缆才能做到。唯一可行的办法只能是由各个监视站分别筛选搜集到的数据。首轮粗筛又称“海量数据规模缩减”（MVR），大约30%的过往数据会在这个阶段被丢弃。[516]在此之后还需要若干轮筛选，丢弃掉绝大多数的无用数据，只留下比较少的有用数据，这样的数据大约有多少呢？国安局和政通局的目标是流量的7.5%。最终这些数据将传回国安局和政通局的数据中心，供情报分析人员使用。

国安局先后开发出了三个版本的“X关键分”系统。由于它们适用于不同的网络条件和不同的任务类型，这三个版本的系统国安局和政通局目前都还在使用。总的来看，大多数系统都安装部署在了执行“时代”计划的那些政通局的监视站点上。

在光缆上搭线搜集到的互联网数据叫作“报文分组”，这是网络协议中比较底层的数据单元。互联网中的每封邮件、每个网页、每段视频、每段语音，在开始传输的时候，都会被拆成若干个一定大小的报文分组，它们在到达终点的时候，计算机系统会根据报文分组携带的信息类别和顺序信息，把它们重新组装起来。

第一版“X关键分”系统试图把所有的报文分组数据都打包成较为高级的会话数据，分门别类但不加筛选。如果数据流量不太大，这一版系统还是足以应对的。政通局以及国安局在许多监视站都使用了第一版系统。不过这一版系统明显存在一个问题：如果数据流量太大，系统就来不及处理所有数据。这边还在筛选，那边等待筛选的数据越积越多，很容易造成系统完全堵塞，导致系统崩溃。为了应对这一问题，“混乱”系统的数据筛选机制就派上了用场。

前面曾经提到，亚历山大局长上台后不久就启动了一个叫作“动荡”的项目，起初不太顺利，但最终还是取得了若干重要成果。其中之一就是代号为“混乱”的一整套系统。这个“混乱”系统可以对以“被动搜集”方式搜集到的光缆、微波和卫星通信数据进行粗略筛选，筛选之后，那些可能有用的数据就被存进了“缓冲区”，等待情报分析人员对它们进行检索、抽取、整理和使用。

“混乱”系统主要根据三类信息筛选数据，第一类是电子邮件或者关键词这样明确的筛选词，第二类是特定的网络或者子网信息，第三类则是带有明确技术特征的信息，例如使用“洋葱头”软件进行通信的数据。一旦有报文分组数据满足这些筛选条件，“混乱”系统就把它们传给“X关键分”，接下来，“X关键分”会把这些分组数据打包成会话数据，分析人员就可以使用这些会话数据了。第二代的“X关键分”系统只在政通局的“肌肉男”计划中使用过。[549]据估计，经过“混乱”系统之后，只有大约5%的数据会传到“X关键分”系统中。

最为先进的第三版“X关键分”系统外号“深潜”，它每秒可以把10吉比特原始数据打包成会话数据，并且使用高级编程语言描述各种筛选规则，更加灵活，也更加强大。可以使用的编程语言有好多种，可以是专用的GENSIS语言，也可以是C＋＋或者Python语言。采用这些编程语言，可以把针对某一类或者某些类数据的规则写成一小段程序，然后根据需要在系统上使用若干这样的小程序。如果有新的一类数据需要被筛选出来，只需要编写针对这一类数据的程序就可以了，这样不会影响到对其他数据的处理。据说，过滤各种数据的小程序有几万个之多。这样一种可以不断叠加新过滤模块的强大系统，国安局和政通局在许多监视站都部署了。[550]

尽管系统对报文分组数据进行了粗筛，丢弃掉了大部分无用数据，但从各种途径获取的原始数据规模仍然巨大。它们只能被分别存储在不同的监视站点上，斯诺登提供的材料显示，国安局和它的“五只眼”盟友大约建立了150个站点和700多个“X关键分”服务器。经过粗筛的数据只能在这些站点待上三天，再经过一轮挑选，一小部分有用的数据会被存进国安局和政通局的数据库里，其余数据则都被滚滚涌来的新数据覆盖掉了。为了让分析人员能够从这些只在站点暂存三天的数据里发现有用数据，国安局使用了一种叫作“联合检索”的技术。某个分析人员从他自己的站点发出查询命令，这个指令会分传给不同的监视站点，让它们分

别在自己存储的那些数据里进行搜索，这些搜索结果最终会返回给发出查询指令的分析人员。“联合检索”是“X关键分”系统的一项重要功能。

要实现快速的检索，必须建立各种各样的索引。为此，“X关键分”系统设计实现了一种灵活的模块化架构，它可以根据需要增加不同的索引项。针对每种索引需求的小程序被称作“插件”。比如，有专门针对电子邮箱的插件，该插件可以把一条会话数据里包含的所有电子邮箱信息都抽取出来，并对域名和用户名建立索引。再比如，有建立完整日志的插件，该插件可以把所有会话数据的网络地址、端口号等信息抽取出来建立索引。还有，可以针对所有客户端数据建立索引，这就更为复杂，可以把接收到的数据包按照类型分开，如图片、文档、动画，或者主机地址、引用地址等，并将其抽取出来建立索引。

有了这些索引，使用“X关键分”可以做的事情就更多了。如果掌握了某个目标的筛选点，比如说他的电子邮箱，或者聊天软件的账号，那么获取他的数据就易如反掌。只要在搜索对话框中输入这些信息，他的最新数据就能源源不断地被看到。如果不知道他的筛选点，也可以借助“X关键分”系统，通过一些不太寻常的情形来缩小查找的范围，最终找到这些筛选点，比如，把使用的语言和居住地不一致的那些人找出来，再看看其中使用加密手段进行通信的那些人，或者看看其中有没有在网上搜索过一些可疑信息的人。

在国安局的一份培训材料里还举了这样一个例子：“X关键分”系统可以利用信息抽取插件对文档和电子邮件内容进行处理，把来自伊拉克的所有包含计算机硬件地址的Excel文件都找出来，这些文件可以帮助情报分析人员绘制出网络地图。

在《卫报》发布的波伊特拉斯拍摄的那段12分钟的视频里，斯诺登说过这样一段话：

当他们想要锁定与外国政府有联系或者与某个恐怖嫌疑人有联系的某个人时，他们就会搜集他的相关通信数据。任何一个情报分析人员都可以在某个时刻、某个地点，使用一个筛选点信息，锁定某个人……我有这样的授权，只要我手里有你或者你的会计师的电子邮箱，我就可以坐在电脑桌前，拿到你们给联邦法官甚至给总统的每一封邮件。[551]

美国政府方面当时对他这段话的回应是完全否认。众议院情报委员

会主席就说："他在撒谎。他说他可以做的这些事情，他根本办不到。"[552]当时只是曝光了威瑞森提交电话记录和"棱镜"计划这两件事情，普通民众对于斯诺登的这番话多半也是将信将疑。直到"X关键分"系统曝光，人们才知道斯诺登所言并非妄语。电子邮件、网络聊天被追踪简直不算什么，就连"魔兽世界"、"第二人生"这样的情境游戏，也被国安局和政通局盯上了，各路游戏粉丝在这些虚拟世界里的一举一动、一言一行都有可能被他们搜集起来，细细分析。[553]

当然，作为普通网民，也有几件可以对抗监视的"防御武器"，比如说"洋葱头"、虚拟专用网络（VPN）以及"安全套接层"协议。而对谷歌这样的公司而言，着力开发出更好的数据保护"武器"则是他们捍卫自己名誉的一场战斗。对国安局和政通局来讲，所有这些"防御武器"都是他们的眼中钉、肉中刺，都是他们日思夜想、想要重点攻克的技术难题。

"X关键分"系统可以识别出使用"洋葱头"等手段保护起来的数据，并且根据需要把它们从其他数据中分离出来，这就为国安局和政通局兄弟俩进一步处理数据创造了条件。在他们令人目不暇接的计划代号中，有两个很有特点，一个是"埃吉山"（EDGEHILL），另一个是"奔牛"（BULLRUN）。

先说说埃吉山。这里是17世纪中期英国内战中第一场战斗的战场，作战的一方是国王的军队，另一方则是议会的军队，当时战况非常混乱，打到最后，谁也没有取得真正的胜利。[494]

再来看奔牛。这里是美国南北战争期间第一场大规模遭遇战的战场。当时，北方军本想速战速决，没想到南方军勇猛反击，最终北方军败下阵来。在"奔牛"之前，国安局把类似的一个破解网络"防御武器"的计划叫作"马纳萨斯"（MANASSAS），这其实和"奔牛"指的是同一场战斗，只不过南方军把这场战斗叫作"马纳萨斯之战"，而北方军则称之为"奔牛之战"。这样一种对名称的反复强调自然引起了大家的好奇。为什么给这个计划起这么一个代号呢？这场战斗首次使用了旗语，双方的信号兵舞动大旗传递信号。因为一方舞旗时，另一方也能看到，所以旗语必须使用密码。有人进一步假设，如果当时北方军能够破解南方军的旗语密码，战局很可能彻底改变。总之，"奔牛"也好、"马纳萨斯"也好，都能和信号情报沾上边。[554]有可能是美国国安局先行启动了"马纳萨斯"和"奔牛"计划，启发了英国人，因此也以他们自己内战的第一场战斗来命名类似的计划。

最直接的密码破译方法叫作“暴力破解”，也就是一点一点去试，可能需要花费很长的时间。不过由于它简单易行，至今仍是一种非常重要的解密方法，这也是“奔牛”计划的重要组成部分。计算速度越快，花费的时间就会更短。为了破译密码，需要计算速度非常快的计算机，它们被叫作“超级计算机”。所以，国安局对于超级计算机一直非常关注。从购买“克雷”一号开始，几乎每隔几年，他们就会购买一台更新更快的“克雷”超级计算机。当超级计算机行业不景气的时候，国安局甚至建立了一个“超级计算机研究中心”，自己制造超级计算机。为了掩人耳目，这家单位被归入美国国防分析研究所（IDA），政府委托研究所的通信研究部门进行管理。[555]

国安局关注量子计算方面的研究其实算不上什么新闻。斯诺登提供的文件显示，国安局正在秘密研制可以用于破译密码的量子计算机，尽管距离能够投入实际使用还需要若干年，甚至有专家认为20年后也不一定能成，可是一旦建成，它的运算速度将比现在最快的计算机还要快得多，按照亚历山大局长的话说，它将是“游戏的改变者”。[556, 557]

在一份预算文件里，国家情报总监克莱伯写道：“我们正在增加在密码分析技术方面投入的资金，希望取得突破，挫败敌方的加密算法，开发利用好互联网流量。”想在密码分析技术方面按照某种预期取得突破，不少专业人士都对此表示怀疑。信息安全专家布鲁斯·施奈尔（Bruce Schneier）就认为，加密算法的数学基础相当牢固，密码分析技术想从这个方面取得突破，可能性不大。他还认为，即使国安局可能拥有了一些比较新的技术，这些技术也不太可能被用于实际当中，去破译各种各样的加密文本。[558]

国安局和政通局想必也知道直接去啃“加密算法”这块硬骨头未必能够成功，所以除了正面攻击，他们还采取了迂回包抄的策略，多路出击，重金开道，也取得了不少进展。政通局在他们内部的文件里就宣称：“那些不知道情况的人会大吃一惊！”过去几年，他们一共攻下了30个虚拟专用网络，他们的目标是到2015年能再攻下300个。[559]面对成绩，他们不无得意地总结道：

过去10年，国安局引领了一个咄咄逼人、多管齐下的项目，破解了广泛使用的互联网加密技术……密码分析技术现在已经上线使用，原本会被丢弃掉的、大量的互联网加密数据，如今都可以被开发利用了。[560]

此言一出，信息安全界马上警觉起来。这仅仅是空穴来风呢，还是确有其事呢？

虚拟专用网络可以使用很多种协议来实现。有人分析，有一种叫作RC4的加密算法可能是整个系统的短板。对于一定长度的密码，只要能够搜集到足够数量使用RC4算法加密的会话数据，就有可能利用统计规律实现破译。对国安局和政通局而言，数据量从来不是问题。[561]RC4算法被广泛用于“传输层安全”协议（TLS）和“安全套接层”协议。这两种协议都可以用来建立虚拟专用网络。除此之外，这两种协议还是广泛使用的超文本传输协议（HTTP）的基础。Wi-Fi应用的有线等效保密协议（WEP）也使用了RC4算法。[561]

若干年前就有专家认为，“点对点隧道协议”（PPTP）也不安全，但许多商业系统仍然在使用这种协议建立虚拟专用网络。相比之下，“互联网协议安全”（IPSec）协议稍微安全一些，国安局想要进入利用这种协议搭建起来的虚拟专用网络，只能通过攻击路由器窃取密码，也就是说，需要动用更多的资源才能完成这件事情。[562]

在国安局密码分析人员眼中，工作难度被分为五个等级。监测一份文件在互联网上的传递路径属于“毛毛雨”，监视脸谱网上的聊天情况是“小雨”，破解俄罗斯的电子邮件服务商传递的加密邮件也仅仅是“中雨”。这些其实都不算什么。[562]

属于“大雨”的工作，包括破解“Zoho”等服务商传递的强加密电子邮件，或者监视使用“洋葱头”软件上网的用户的情况，再有就是破解使用“无痕迹”协议加密的聊天信息。原本还有一种叫作“TrueCrypt”的软件也属于“大雨”，斯诺登曾在他主持的草根密码晚会上专门介绍过它，可惜，在2013年5月，开发人员宣布迫于政府压力，他们将不再更新这个软件。[562]

如果有人把“洋葱头”软件、“CSpace”聊天软件和“ZRTP”网络电话软件组合到一起，那就成为国安局最麻烦的“灾难”。对国安局而言，这些人在什么地方、聊了什么，几乎完全不可知了。[562]

加密算法总是通过软件来实现的。即使理论上没有问题的算法，也可能由于软件制作方面考虑不周而造成安全方面的漏洞。有一种被许多网站用来加密数据流的OpenSSL软件，就被发现存在一个漏洞，并非加

密过程有问题，而是处理加密连接时有瑕疵，但由于瑕疵处于OpenSSL软件的核心，这个漏洞被认为是“安全套接层”协议应用过程中最严重的问题，并且已经存在了至少两年之久。人们怀疑，国安局在这个漏洞公开曝光之前就已经掌握了这一情况，并且在充分利用它搜集情报。[563]

这种怀疑并非毫无根据。据调查，就在2012年9月，国安局跟一家叫作“维尤彭”的法国公司签了一份为期一年的合同。这家公司的主营业务就是出售“零日”（zero-day）漏洞。所谓“零日”漏洞，就是尚未被软件开发商自己发现的那些漏洞，因而没有针对这些漏洞的补丁程序。利用这些漏洞，国安局就可以绕过对方预设的安全机制，拿到他们想要的数据。[564]不过获取这些漏洞可一点儿也不便宜。有报告称，国安局每年给另外一家叫作“终局系统”的公司支付250万美元，得到的只是25个“零日”漏洞。[344]

对此，国安局局长亚历山大是这样解释的：

国安局必须理解并掌握技术工具里的所有漏洞——编程错误、后门以及“零日”漏洞等，我们的国家依赖这些工具保护系统安全，使其免遭对手染指。[565]

专家建议奥巴马总统对国安局提出要求，一旦他们发现软件中存在重大安全漏洞，必须公布出来，以便工作人员及时打上补丁。总统基本上同意了他们的意见，只是增加了一个小小的例外情况：如果这个漏洞的确可以用于国家安全或者执法，那就可以对它秘而不宣、悄悄利用。[566]

第八回 大数据

就在“9·11”事件发生之前两个月，国安局局长海顿接受了一次媒体采访。针对社会上流传的国安局已经落后、越来越聋的说法，他说：

由于现代通信的规模（Volume）、类型（Variety）和速度（Velocity）的发展，以电磁频谱为主要工具的信号情报单位，面临着被大量信息淹没的危险。因此，与其说变聋，还不如说是被数据的海洋淹没。现在我倒承认，被淹没的结果就是变聋了。从大量的通信数据中把有价值的情报挑出来十分困难。[567]

局长这段讲话里的几个“V”非常醒目。时至今日，但凡有关“大数据”的演讲和报告，几乎都毫无例外地提到“规模”、“类型”和“速度”这几个词。不过这三个“V”并非局长个人的发明。2001年3月，在另外一次媒体采访中，信号情报分局的负责人莫林·巴津斯基（Maureen Baginski）表示，在信息时代，国安局面临的最大问题是数据太多，掌控数据的规模、速度和类型都成为问题，要理解这些数据非常困难。[568]

2002年10月，面对参众两院情报委员会联合调查组，海顿局长再次表达了他的苦恼和关切：

三年前，在我第一次和国会议员们开会的时候，他们告诉我，国安局已经落后，面临边缘化的危险。最严峻的是技术方面的挑战。人类通信的规模、类型和速度，使得我们完成任务日益困难。[569]

对国安局而言，“规模”、“类型”和“速度”这三个词的含义很明确。对此，技术专家宾尼是这样解释的：

规模意味着你有更多的数据可供检索，可以从中找到更多与目标有关的数据；速度意味着你得到数据的速度更快；类型则意味着你可以得到关于目标的更多方面的数据。[570]

和海顿局长英雄所见略同的还有一位，他也有着很好的教育背景，也是非常优秀的高级技术军官，同时也是一名将军。不同的是，海顿来自空军，他来自海军，并且比海顿年长10岁。此人名叫约翰·波因德克斯特（John Poindexter）。

2002年3月25日，海顿在自己的办公室里接见了波因德克斯特，这是两个人第一次也是最后一次面对面。整整7周之前，波因德克斯特曾经来过一趟国安局，那次接见他的是常务副局长布莱克。[571]这位布莱克正是被局长钦点，却让“开拓者”项目以失败告终的监管人。

波因德克斯特访问国安局的目的很简单——推销他主持的一个重大项目，这个项目有一个响亮的名字：“全面信息感知”（TIA）。

老将出马

先把时间调回1999年。

在这一年的美国国防高新局的技术年会上，信息系统办公室的项目经理布赖恩·沙基（Brian　Sharkey）做了一个报告，题目是“全面信息感知”。尽管其中涉及了已经在进行的一些项目，但总体上看，那还只是他头脑中的构想，并非一个已被批准的计划。[572]

他首先介绍了两种战争形态：一种是对称的，传统的国与国之间的战争都是这种形态，参战双方很清楚对手是谁；还有一种是非对称的，参战人员相对而言很少，也很不容易确定对方的情况，经常采用非常规的战术，而且往往会产生巨大的影响。[572]

沙基认为非对称作战的挑战在于：因为可能参战的目标实在太多，想要在冲突爆发之前较早分辨出哪些是真正的对手、哪些不是非常困难。想要做到这一点，就必须全面搜集有关他们的数据，利用这些数据进行判断。越早确定冲突目标，就越有可能缓解甚至阻止冲突的发生。最后，他介绍了正在进行之中的“前帆”（GENOA）项目，这个项目只是他的“全面信息感知”构想中很小的一个部分。他说，处理危机的过程中会有很多不确定性。面对同样一组数据，可能会建立起多种假设，这就需要建立一个协同的环境，让人们集体进行推理，高效并且有效地帮助他们对各种数据取得共识，或者清晰地向决策者陈述分歧。这是“前帆”项目的出发点和落脚点。[572]

这个“前帆”项目的负责人就是波因德克斯特。对大多数人而言，这是一个非常陌生的名字。对现在二三十岁的年轻人而言，更是如此。说到他，就必须提到“伊朗门”事件（Iran-Contra Affair）。

“伊朗门”事件是20世纪80年代美国政治生活中的一个重大事件，是可以和“水门”事件相提并论的另一次重大政治丑闻。已经有很多人专门围绕这件事情写了好几本书，由于它在这一回故事里会被反复提到，所以还是有必要尽可能简单地说上几句。

美国和伊朗是一对死敌，但为了营救被黎巴嫩真主党绑架的美国人

质，里根政府秘密地与伊朗政府接触，想卖一些伊朗急需的军火给他们，以换取人质的自由。这一切交易绕过了国会。伊朗支付的货款并没有回到美国，而是被秘密转移到了其他地方，其中一个地方是尼加拉瓜的反政府游击队。这一切操作再次绕过了国会。但是，“没有不透风的墙”，这大概是“放之四海而皆准”的一条真理。事情没过多久就被曝光出来。波因德克斯特，当时是里根总统的国家安全事务助理，知道并操控了整个过程。在随后的国会听证会上，他只能以“不记得”三个字搪塞——他别无选择。但法院还是找到了许多确凿的证据，他被判重罪，万幸的是，他最终因为证据方面的技术性原因没有实际服刑。这一过程是相当长一段时间内美国电视和报纸上的热点新闻。波因德克斯特最终在一片谴责声中告别政坛，接替他的人名叫卡卢奇。

远离政治旋涡的波因德克斯特生活平静，即使什么都不干，靠着丰厚的退休金也可以衣食无忧。不过他是闲不住的，在一家小小的咨询公司工作之余，他竟然自学了好几种计算机程序语言，甚至还设计了一个用于检查软件代码错误的小程序。时间不知不觉到了1995年，这一年他59岁。一个老同学突然找到他。这位同学在一家叫作“新泰”的公司里工作，这次跟他联系是想请他帮公司争取一个国防高新局的信息技术项目——“大三角帆”（SPINNAKER）。[573]

波因德克斯特一下子就来了精神。很快，他就见到了国防高新局负责这个项目的主管。没错，就是沙基——他也来自海军。沙基大致讲了他的想法。他想建立一个多人协作的系统，以便访问若干个独立的数据库，目的是帮助富有经验的决策人员，克服由于数据过多过乱而带来的麻烦，从而对未来的灾难做出预测。波因德克斯特太熟悉这个想法了。10年前，在事后分析贝鲁特兵营遭遇爆炸袭击原因的时候，他就产生过类似的想法。因此，这个“大三角帆”在沙基头脑里虽然还只是一个模模糊糊的想法，但在波因德克斯特那里已经呈现出比较清晰的图景。[573]

会谈结束，新泰公司拿到了项目合同，波因德克斯特也得到了公司资深副总裁的位置。沙基琢磨着给他的“大三角帆”起一个新名字，代表这个项目进入了新的阶段。他绞尽脑汁想出来的是“危机协同理解与管理系统”，然而这名字过于直白，显示不出其分量。最后还是由波因德克斯特出手，项目的新名字就叫“前帆”，船在逆风航行时靠的就是这面帆。[573]

“9·11”事件之后的第二天，沙基突然接到一个电话，是老朋友波因德克斯特打来的，希望能马上见个面。两个人在一处安静的地方碰了头，谈话中提到情报安全部门未能提前制止袭击发生。波因德克斯特告诉沙基，他相信一定能在技术上找到一整套方法，为情报分析人员提供更好的数据和更快的通信网络，以及能帮助他们更清晰地思考问题的计算机程序。可以参考沙基两年前提出的“全面信息感知”构想，建立一套全新的系统，从互联网这样的开放信息源，以及政府和私营数据库中收集信息，不间断地扫描数据，从中发现恐怖分子的蛛丝马迹。简而言之，就是为有效监视和预警恐怖活动提供尽可能高级的自动化手段。两人一拍即合。[574]

沙基很快就把刚刚上任几个月的国防高新局局长安东尼·特瑟（Anthony Tether）约了出来，专门向他介绍“全面信息感知”构想。沙基上次介绍这个构想的时候，特瑟正开着一家不大的公司，自任董事长兼总经理，有滋有味地做着自己的生意。沙基最后说：他提出这个想法后不久就离开了高新局，这件事情也就搁置下来。现在，这种想法正当其时，应该加紧推进。特瑟被他说服了：

太棒了！我们必须这么做。我们需要建立一个办公室，你来牵这个头。我们必须重新启动这个项目[574]。

这时沙基却犹豫了，他的话很实在：

我要供两个孩子上学，这需要一大笔钱。在他们完成学业前，这件事情我干不了。[574]

特瑟开出了他能支付的最高薪水，但沙基仍然觉得落差太大，他此时是科应公司的高管，同时也是公司的股东，公司的效益很好。两个人商量的结果是：请波因德克斯特出山。波因德克斯特其实也有些犹豫，因为他10多年前深陷“伊朗门”事件丑闻，公众形象不佳。考虑再三之后，他同意走马上任。他说：

我了解技术，也理解情报问题和决策过程，我有很多办法把这三样东西捆绑成为一个整体。[574]

为了请波因德克斯特出山，特瑟局长表现出了巨大的诚意：他开出的年薪高达138200美元，虽然比波因德克斯特在新泰公司147182美元的年薪稍少了一些，但这已经是国防高新局里最高的年薪水平了，局长

自己也就拿这么多。[575]

重启“全面信息感知”

2002年2月，新的信息感知办公室刚成立一个月，《纽约时报》记者约翰·马可夫（John Markoff）就把这个办公室披露了出来，并且告诉世人，当年“伊朗门”事件的主角之一波因德克斯特现在是这个办公室的负责人，还顺便把他的另一段负面往事也搬了出来。1984年作为里根的国家安全事务副助理，波因德克斯特主持制定了《第145号国家安全决策规定》，该规定授权国安局检查政府计算机系统里是否存有“敏感但非密的信息”。后来，波因德克斯特把这项授权进一步扩大，允许国安局检查私营企业的计算机和通信安全。[576, 577]这些在当时都引起了不少非议。

波因德克斯特似乎并没有把马可夫的这篇文章放在心上。他这段时间主要在考虑一个问题：如何劝说美国情报圈子里的那些主要单位参与到他的项目中来。2月2日访问国安局的时候，对方安排了整整一天的活动，布莱克副局长几乎陪了他一天。不过副局长主要是听，话并不多，更没有明确表态。但他的这种态度还是让波因德克斯特备受鼓舞。副局长的口风很紧，他并没有把国安局正在大张旗鼓进行的“开拓者”项目告诉波因德克斯特，也没有透露正在秘密进行的“星风”行动的任何相关信息。但波因德克斯特是何等聪明，他敏锐地感觉到国安局情报搜集的规模比以往扩大了很多，他的“全面信息感知”正是他们最需要的东西。[571]

除了国安局，在波因德克斯特的走访清单上，还有一些重要人物。国安局前局长麦康奈尔就是其中一位。尽管麦康奈尔比自己年轻几岁，波因德克斯特却对他的才干很是敬佩，再加上他也是一名海军将军，更增加了几分亲切感。[578]

两个人见面的地点是麦康奈尔在博艾汉公司的办公室。前文已经说过，麦康奈尔在1996年从国安局局长的位置退下来后就旋转进了这家公司，成为开拓公司情报领域业务的高管。对于波因德克斯特正在推行的这个“全面信息感知”计划，麦康奈尔已经有所耳闻，他直言不讳地提醒波因德克斯特，政治上的大麻烦才是麻烦。“全面信息感知”最终想要建立的是普通民众的档案，但如果大众和国会了解到这一情况，对这个计

划和波因德克斯特本人都将是一场灾难，而最厉害的杀手是那些国会议员。[578]

对于这些，麦康奈尔已经有所准备。他告诉波因德克斯特，自己愿意出面去找国会里的重要人物，取得他们的关照和支持。他还提醒说，千万不要把“全面信息感知”描绘成一个针对美国国内的情报计划。相比之下，麦康奈尔对于情报监视相关法律规定的认识要比波因德克斯特等人成熟和现实得多，由他出面去做通国会层面的工作，扫清“全面信息感知”发展的道路，波因德克斯特求之不得。[578]

当然，麦康奈尔做这些事情并非一无所求，他不仅是个清醒的政客，更是一个精明的商人。国安局前局长马上开出了自己的价码：他希望波因德克斯特把整个“全面信息感知”计划的所有合同都交给博艾汉公司。波因德克斯特显然懂得“不能把所有鸡蛋都放进一个篮子”的古训，他拒绝了麦康奈尔的请求。看到对方面露失望，他加了一句：“我还是很希望你们能够参与这个计划。”最终，博艾汉公司拿到了总额超过800万美元的合同。[578]

特瑟局长在审批合同的时候，看到其中包含了寻求国会关照的一些条款，他大笔一挥删掉了这一部分。他告诉波因德克斯特：“我们不需要这个。”波氏告诉局长，国防高新局需要利用麦康奈尔的影响力推动计划顺利进行，可惜局长不为所动。局长对“全面信息感知”即将面临的政治问题根本不重视，这一点让波因德克斯特颇为担心。他知道，如果这个计划有朝一日真的遭到质疑、攻击甚至被否定，他所能依靠的就只有他自己了。[578]

5月，“全面信息感知”的第一阶段试验开始。随后每进行一轮试验，波因德克斯特都会拿出更多的工具，其中一些还不错，另外也有一些并不怎么样。到2002年年底，他的“全面信息感知”试验网络里已有250个节点，其中国安局最多，安装了15个节点。不过他却发现一个非常奇怪的现象，国安局只是安装了试验节点，并没有参与任何一次试验。他事后才知道，国安局悄悄地把试验节点上的各种工具都搬到了他们自己的网络上。可他们很快就失望了。因为那些工具都还处于试验阶段，充其量只是原型系统，把它们直接当作工作系统，实时处理国安局从各个渠道获取的大量数据，肯定是不行的。[579]

在8月召开的国防高新局技术年会上，波因德克斯特继续慷慨陈

词：

我在白宫工作的时候，确定情报搜集目标是一件比较容易的事情。有时候得到情报很困难，但目标很明确。现在，我们处于一个非对称的世界。美国面临的最严重的非对称威胁是恐怖主义，这种威胁的特点是敌人松散地存在于隐蔽的网络之中，难以确定……情报搜集的目标是成百上千的人，他们的身份和行踪我们未必掌握。

我们必须更加高效、更加聪明地发现新的数据源，从新旧数据中挖掘信息，利用这些信息进行分析，把它们转变为知识，产生可以执行的行动方案。

国防高新局信息感知办公室就是要为我们的安全和隐私创造出新的技术。除了让不同的数据库互联互通，我们需要找出更好的方法从集成的数据库中抽取信息，同时保证清白公民的隐私信息得到保护。

要解决这些问题，需要各种各样的工具、方法和过程，但它们必须利用一个公用的系统架构集成起来才能发挥作用。我们的答案是全面信息感知原型系统。有待挖掘的一种新的重要的数据源是交易活动信息空间。恐怖组织策划和实施对美国的攻击，这些组织成员必须进行一些交易，他们必然会在这个信息空间里留下蛛丝马迹。……我们必须从噪声数据中把这些蛛丝马迹找出来。[580]

交易活动信息空间里有哪些数据呢？波因德克斯特并没有接着往下说，但有一张幻灯片配合他的发言，再加上信息感知办公室的另一张幻灯片，两者清晰地罗列了这样一些内容：财务数据、教育数据、旅行数据、医疗数据、交通数据、出国数据、活动数据、位置数据、住房数据、通信数据等，可以说涵盖了普通美国人生活的方方面面。

波因德克斯特的“全面信息感知”计划基本上继承了沙基的“全面信息感知”构想的主要元素，范围更为明确，表达更为浅显易懂，更接近于工程现实。例如，对于“全面信息”的范围，沙基用了一个比较笼统的“信息空间”概念，波因德克斯特则比较明确地将其限定为“生物验证识别数据”和“交易数据”两类；而对于依赖“全面信息”建成的数据库，沙基用的是比较抽象的“索引空间”概念，而波因德克斯特则使用了较为具体的“自动虚拟数据仓储”等。沙基通过这些模糊的、笼统的、抽象的概念包装“全面信息”，普通民众未必能理解其中的真实含义，而波因德克斯特

把“全面信息”解释得如此清楚明白，他的“小伙伴们”一下子就理解了，也顿时惊呆了。

以现在的眼光回顾这件事情，不免产生这样一种感叹：波因德克斯特到底只是一个技术出身的“专家”，他有点儿太实在了。他采用的是“生物验证识别数据”和“交易数据”这两个让人感觉不太舒服的、技术性比较强的概念，如果再大胆一点儿，找一个或者干脆创造出一个技术性不太强但是更炫更酷的新词汇来包装“全面信息”，情况会怎样呢？这个新词在若干年后被别人构想了出来，叫作“大数据”。

20年前，波因德克斯特本人曾经吃过“通信数据”很大的苦头。1981~1983年，他参与了白宫危机管理中心（也被称为总统紧急行动中心）的现代化改造计划，引入了在当时非常先进的一种工具——电子邮件。在“伊朗门”事件过程中，他被发现曾故意删除了大约6000条相关信息。波因德克斯特百密一疏，没想到这些被删除的电子邮件都被他自己精心设计的备份系统保存了下来，其中一些脱机备份成为法院调查的证据，证明他在国会反反复复念叨的三字经“不记得”是在撒谎。他最终被认定犯下的重罪包括：在国会撒谎、销毁有用文件、妨碍国会调查等。[581]尽管后来他得到豁免没有去蹲监狱，但这无疑成为他永远无法抹去的一大历史污点。

波因德克斯特早年以优异成绩毕业于海军学院，和参议员麦凯恩是同班同学。麦凯恩曾在2008年跟奥巴马竞争过总统宝座，斯诺登对他颇有好感。波因德克斯特后来进入加州理工学院学习，最终拿到了核物理专业的博士学位。给波因德克斯特上过课的老师包括1961年获得诺贝尔物理学奖的伦道夫·穆斯堡尔（Rudolph Mössbauer），而他的博士论文评阅小组成员竟然包括1965年获得诺贝尔物理学奖的理查德·费曼（Richard Feynman）。[574]这就是加州理工学院，全球范围内为数不多的、仍然坚持“理工学院”这种低调名号的声誉卓著的学校！我国著名科学家钱学森和徐璋本都是这个学校的博士。钱学森后来回忆说，在这里的学习使他“一下子脑子就开了窍”。[582]可能正是因为波因德克斯特具有很高的学习天分、技术素养和信息科学素养，这导致他发自内心地看不起媒体记者、国会议员、检察官和法官，也导致他敢于“冒险”去做违法的蠢事，以至于酿成大错。

在国防高新局的这次技术年会上，“全面信息感知”计划的主要项目纷纷登台亮相。

首先上台的是“前帆（二期）”。对这个项目前一期的情况，波因德克斯特是再熟悉不过了的，因为他在新泰公司的几年时间里，主要做的就是这个项目。简单地说，“前帆”的实质是建立协同环境，为某个工作团队的信息发现、系统推理和知识复用提供必要的技术手段，但当时只是解决了“有无”问题，协同系统的整体性能和效果都还不够理想。“前帆（二期）”要通过提高数据搜集、数据组织和可视化等项目的自动化程度来改善性能；要开发出现状建模、未来预估、风险分析、备案提供等工具，使“全面信息感知”协同环境变得更为“灵巧”；还要支持中心模式和边缘模式两种协同方式：中心模式紧密协同，共享数据和服务器，而边缘模式则松散耦合，灵活建立专网进行协同。[583]

接下来是新上马的项目“创世纪”（GENISYS）。这个项目的目的是开发出一种数据聚合技术，能够集成各种已有的异构数据库，容纳各种媒体类型的数据，而且从架构上来说应该是分布式的，规模伸缩性要好。[584]结构化数据库满足不了这些要求，所以这应该是一种半结构化甚至非结构化的架构。之所以提出这样的要求，是要在最大程度上为后面的数据挖掘和信息分析过程提供一种看起来规整、似乎是集中式的数据库，用专业一点儿的术语来说就是“虚拟聚合”（virtual aggregation）和“逻辑集中”（logical centralization）。[585]

第三个登场的是“证据抽取和关联发现”（EELD）。这个项目最能体现数据挖掘的意思：要能从大量数据中发现人员、事物、机构、地点之间的关系，并且能把一点一滴的信息串接起来形成特征模式，还要能根据这些模式区分出哪些是正常、正当的行为，哪些是恐怖分子的行径。[586]这个项目所要求的数据挖掘模式与商业企业的数据挖掘模式有所不同，商业企业侧重于从大量数据中发现一些普遍存在的“规律”，例如某些客户买了A，又买了B，那么和他们根本没有任何关系的客户也可能如此，而情报分析则更希望从数据中发现某些罕见但重要的异常情况。[585]

三个翻译类项目“跨语言信息探测–抽取–摘要”（TIDES）、“有效–实惠–可复用的语音到文本转换”（EARS）和“巴比伦”（BABYLON）被放在了最后。这些项目是希望把监听到的各种语音通信数据转换成文本，再把不同语言的文本自动翻译成英语。在幻灯片上，清晰地和阿拉伯语并列在一起的居然是中文。处理阿拉伯语的信息和数据很明显是为反恐战争做准备，那么为什么会处理中文数据信息呢？[587]

这次技术年会是波因德克斯特退出政坛后的第一次高调亮相。会上展示的这些系统和构想从技术上讲都是很耀眼的，可是有些细心的人发现，其中没有涉及一丝一毫的隐私保护，也没有强调这些系统仅用于对外情报，不针对美国国内。相关人员更没有听从麦康奈尔的建议，强调这些系统只是演示验证系统，并非工作系统。波因德克斯特没有意识到，麦康奈尔的一些担心很快就会变为现实，同样，他也没有察觉到，马可夫的那篇文章引起的负面关注和反响正在逐步汇聚，正在从和风细雨变成狂风暴雨、从涓涓细流变成惊涛骇浪。他即将面对的是记者们打出的“组合拳”：第一招清算旧账，第二招抹黑形象，第三招全面否定。他怎么也想不到，“全面信息感知”最终会败在这套组合拳之下。再加上一些国会议员的加入，他根本没有任何还手的机会。

轮番发难

2002年11月，可能是波因德克斯特几年来最难熬的一个月。《纽约时报》《华盛顿邮报》等美国主流媒体接连刊登重磅文章，严厉抨击“全面信息感知”计划。

首先是11月9日，《纽约时报》的马可夫再次发难。他2月的那篇文章只是提到了信息感知办公室，而这一次他的火力集中到了“全面信息感知”计划上，当然也不会放过波因德克斯特。

国防部正在开发一个计算机系统，布下一张巨大的电子天罗地网，在全球范围内（也包括美国）搜索个人信息、追捕恐怖分子。

作为这个系统的负责人，波因德克斯特中将在五角大楼的文件和发言材料中是这样说的：利用这个系统，情报分析人员和执法人员无须搜查令，就能立刻得到公民个人的电子邮件、电话记录、信用卡记录、银行交易记录、旅行记录等信息。

今年1月，波因德克斯特将军悄无声息地回到政府，执掌国防高新局的信息感知办公室，这间办公室专门负责在“9·11”事件后开发新的监视技术。

为了部署这个“全面信息感知”系统，我们需要新的法律，其中一些内容已经在小布什政府提交给国会审议的《国土安全法案》中有所体现。1974年颁布的《隐私法案》就是要限制政府部门搜集使用隐私信息的行为，新法律将对这部法案进行修订。[588]

波因德克斯特看到“中将”“将军”这些称呼的时候，一定会有种芒刺在背的感觉。“伊朗门”丑闻曝光之后，他无法继续在白宫待下去了，只能灰溜溜地回到海军部，去当海军作战部部长的助手。这很可能只是个名义上的虚职，并不需要他实际做什么事情。但他的军衔实实在在地从中将降为少将。[589]这肯定是个令人很不舒服的位置，从一开始就注定不可能让他待太长时间，不久他就光荣退休了，那一年他刚刚51岁。

为了增强自己文章的可信度，马可夫还专门请来了专业人士为自己

助阵。

曾经担任美国计算机协会主席的巴巴拉·西蒙斯说："对于这个系统，我的许多同事都感觉很不舒服，并且对这项技术的潜在用途表示忧虑，因为即使不是现在的这个政府部门用，将来它也会被另一个政府部门使用。一旦你部署了这个系统，你就不可能控制它了。"[588]

马可夫的文章登出后三天，《华盛顿邮报》的罗伯特·奥哈罗（Robert O'Harrow, Jr.）就扑了上来。他写道：

波因德克斯特说，任何一个运行的系统都将包含防护手段，对信息搜集过程进行控制。他还说，软件中内置了用户识别、跟踪审计、信息控制的规则。但是他说，他的任务是技术开发而不是制定政策，这些问题需要由国会和政策制定者决定，由他们为系统建立起政治底线。[590]

接着，奥哈罗把波氏在"伊朗门"丑闻中欺骗国会的往事点了出来，意思很明显：这个人在历史上就不诚实，现在是不是"逗你玩儿"，你自己想吧。

在文章的结尾，奥哈罗写道：

信息感知办公室把美国国徽稍作改动就变成了自己的图标：金字塔上赫然装上了一只眼睛，它似乎正在扫视这个世界。[590]

又过了两天，《纽约时报》登出了威廉·萨费尔（William Safire）的一篇煽动性和火药味十足的文章。此人曾经做过前总统尼克松的讲话撰稿人，开篇他就为美国人描绘了这样一幅场景：

每次你用信用卡购物、购买杂志、支付药费，你访问的每个网站、收发的每封电子邮件，你的每个学习成绩、每笔银行存款，以及你预定的每次旅行和你参加的每个活动，即你所有的交易活动和交际活动，都存进了国防部所说的"一个虚拟的、集中的、庞大的数据库"。

从各种商业来源得到关于你私人生活的计算机化档案，再加上政府已经掌握的你的每条信息——护照、驾照、过桥缴费记录、诉讼和离婚记录、对喧闹邻居和联调局的抱怨、你出生以来的各类书面证明材料以及最新的隐蔽的监视录像，这就是那个超级窥探者的梦想：对每个美国

人进行“全面信息感知”。

这距离奥威尔描绘的场景已经不太远了。如果波因德克斯特得到了他想要的、史无前例的权力，不出几个星期，这些都将在你的生活中发生。[591]

萨费尔给波因德克斯特扣上了一顶“超级窥探者”（supersnoop）的大帽子，然后把波因德克斯特希望大家彻底忘记的往事又回顾了一遍，接着他说：

波因德克斯特正在实现他种下了20年的梦想：获得“数据挖掘”的力量，对每个美国人的公开的和属于隐私的行为进行秘密监视。

匆忙之中通过的《美国爱国者法案》扩大了《外国情报监视法案》的适用范围，削弱了15部隐私法律，即便如此，它仍然要求政府向国会和法院报告秘密监视的情况。但波因德克斯特粗暴践踏了这些监管措施，严重威胁了个人隐私。[591]

最后，和奥哈罗类似，萨费尔也狠狠地踹了信息感知办公室的图标一脚。他说：

波因德克斯特的新办公室的拉丁铭文是“Scientia Est Potentia”——“知识就是力量”。更准确地说，就是政府掌握的有关你的无限知识，就是它凌驾于你之上的力量所在。[591]

这些文章被美国内外媒体广泛转载，把这一轮口诛笔伐运动推向了高潮。接下来的几天，波因德克斯特被新闻媒体包围了。所有主流媒体都想采访他，各大电视台也想请他上节目，不过大都有些不怀好意。“伊朗门”丑闻以及更多旧账被翻了出来，人们一遍又一遍地从道德层面对他进行拷问，总结起来就是六个字——“此人绝不可信”。他们说，在波因德克斯特负责建立白宫早期的电子邮件系统过程中，他特意设计了一个秘密的“后门”，叫作“隐私免检”，专门用以对付正常的检查监督，这也成为他在“伊朗门”事件中进行幕后指挥控制的信息隧道。所以密歇根大学信息学院的专家评论说，

波因德克斯特故意采用这种聪明的方式操控系统、隐藏信息。一旦面对监督和检查，他就决定采取非法行动。由这种人负责设计系统，对美国公民进行有史以来最全面的监视，这将意味着什么呢？[581]

“全面信息感知”计划对美国普通民众产生恶劣影响的可能性被逐渐放大，从美国人最关心的个人隐私保护的层面进行拷问，总结起来也就是六个字——“此事绝不可为”。

也有人站出来反驳，替“全面信息感知”计划鸣冤叫屈。传统基金会的迈克尔·斯卡达威利（Michael Scardaville）就是其中之一，他写道：

事实上，“全面信息感知”计划正是“9·11”事件之后公众、国会和决策者所需要的：把零碎的片段拼凑成完整的恐怖行动拼图，阻止下一场“9·11”事件的发生，同时保护美国人的公民自由权。

尽管为每个美国人都创建一份档案可能有助于调查恐怖分子的行踪，但这种做法能够为反恐战争提供有用信息的概率实在太小，所以这并非“全面信息感知”的设计目的……这个系统只是要更加高效地利用已经存在的信息而已。利用这样一种技术，情报界可以对某个恐怖嫌疑人建立起比较详细的档案，其中包括他经常联系的对象信息和经常参加的活动信息。[592]

对于“全面信息感知”系统的使用，他建议说：

这个系统一旦建成并且部署使用，就必须制定政策严防其被滥用。最重要的原则是，它的使用应该被限定在预防未来恐怖袭击的情报工作范围之内……这种强大的工具应该只能由承担反恐任务的那些情报单位使用，例如中情局、联调局以及新成立的国土安全部的情报部门。如果这些单位的人员滥用这一工具，也应该严惩不贷。[592]

从后来者和旁观者的眼光来看，斯卡达威利的这篇文章并非一无是处，其中有些观点还是比较理性、比较客观的，但他的文章只发表在基金会自己的网站上，因此传播面和影响力有限，而且他建议“全面信息感知”系统应该由中情局、联调局等情报单位使用，通过建立配套的政策进行约束，这大大削弱了他这篇文章的力度，普通民众看到这篇文章，他们的疑虑和困惑不仅不会消除，而且还有可能更甚，因为这些情报单位过去都做过一些不干不净的事情。

媒体记者用奇谈怪论博人眼球或煽风点火搅动民意并不算出格，但有人想到了“以其人之道还治其人之身”这一招：你波因德克斯特不是要对我们普通民众“全面信息感知”吗？我们就先把你的信息“全面感知”出来：旧金山的一家杂志社“感知”到了波因德克斯特的电话号码和住址，

并马上把这些信息公布出来，更有甚者煽动大家打电话扰乱那一家人的日常生活。[593]这样做就太过分了。

波因德克斯特显然感受到了来自各方的强大压力。在某些场合，他对信息感知办公室的图标进行了解释：图标上的那只眼睛是由谐音而来，代表了字母“I”（英文中“眼睛”一词的读音与之相同）；金字塔和地球则是由形状而来，分别代表了字母“A”和“O”，合在一起就是信息感知办公室的英文缩写“IAO”。[581]当然这只是他的一面之词：不管大家信不信，反正他是这样说的。不过没多久他就撤掉了这个惹事的图标。

败走麦城

国会议员出手了。很快，波因德克斯特就不得不坐在50多个议员和他们的助手面前，进行专题汇报。他准备了一份长达三个小时的材料，可刚刚汇报了15分钟，听众就开始有些不耐烦了。“嘿！你打算什么时候才开始谈今天汇报的目的？”有人站了起来，打断了他的汇报。波因德克斯特吃了一惊。“讲数据挖掘！”对方接着说道。波因德克斯特解释说，为了让大家更好地理解，他必须先把背景交代清楚，他接下来会讲清楚隐私保护问题。可是对方说，他想马上知道答案。波因德克斯特终于按捺不住了，他厉声说道：“你坐下！我会讲这个问题，但是至于我先讲什么、后讲什么，不用你指手画脚！”[594]

这样一次火药味十足的会议，其结果可想而知。参议院财经委员会主席查尔斯·格拉斯利（Charles Grassley）提出，国防部总监察官应该对“全面信息感知”计划进行全面评估。对这个计划步步紧逼、连下重手的是参议员怀登。他先是和菲因高德一起提出：在国会调查这个计划之前，应该停止资助有关的项目。这一提案在2003年1月获得通过。[595]紧接着，怀登又提出一项提案：国防高新局必须提交有关这个计划的详细报告，时间期限是90天。他的这个提案也获得了通过。[596]

一番忙碌之后，波因德克斯特还真在90天内拿出了报告，把已经引起误解的“全面信息感知”改成了“反恐信息感知”（英语缩写仍然是“TIA”）。新计划包含的内容更丰富，可细分为四个专题：

第一个是协作和决策支持专题，包括“前帆（二期）”、“非对称环境兵棋推演”（WAE）、“快速分析型兵棋推演”（RAW）和“未来预测市场”（FUTUREMAP）四个项目。

第二个是外语翻译专题，包括“有效–实惠–可复用的语音到文本转换”、“跨语言信息探测–抽取–摘要”、“全球自主语言开发”（GALE）、“巴比伦”和“交响乐”（SYMPHONY）五个项目。有时候，前面三个项目也被统称为“多语种语音和文本自动开发”。

第三个是数据搜索、模式识别和隐私保护专题，包括“创世纪”、“证据抽取和关联发现”、“误报探测”（MINDET）、“可扩展的社交网络分

析”（SSNA）、“远距离人物识别”（HUMANID）、“运动–识别–监视”（ARM）、“下一代人脸识别”（NGFR）和“生物事件首要指标识别技术”（BIO-ALIRT）共八个项目。

第四个是总集成专题，任务很明确，就是把上述工具集成到一起，建立信息感知原型系统。[597]

需要说明的是，上面提到的这些项目大多在“全面信息感知”计划启动前就开始运作了。波因德克斯特的思路很明确：尽量利用国防高新局已经开展的项目所取得的成果，打造出一个能够全面感知反恐信息的原型系统。看着这份100多页的报告，他颇为得意，这是很长一段时间以来他自己写的最满意的一份材料了。[598]

但怀登参议员不这么看。在他眼里，这份报告是很不让人满意的：

计划的名字虽然改了，但是很明显，原有的计划框架并没有改变，仍然要搜集个人信息、进行模式分析……绕开程序性的保护措施，把守法的美国公民确定为恐怖嫌疑人。[599]

更让波因德克斯特始料未及的是，他的这份报告不仅没有消除怀登等人的疑虑，还给他们提供了现成的炮弹。在报告的附录里，议员们有了一个新发现。7月28日怀登组织召开了一次新闻发布会，靶子很明确，“未来预测市场”。这是“反恐信息感知”计划中的一个比较小的项目，设立于2001年5月，它最早也不是这个名字，而叫“基于电子市场的决策支持”，比“信息感知办公室”成立以及“全面信息感知”计划启动还要早一年多的时间。这个项目采用了一种近似于股票市场的方式来预测将来可能发生的事情。有两家单位获得了项目资助，其中一家是“网络交易”公司。这家小公司是由加州理工学院的约翰·利亚德（John Ledyard）教授创建的，他转手把项目分包给了乔治·梅森大学的两个教授，建立了一个“政策分析市场”的网站，打算每个季度都公布若干事件供大家预测，但最终似乎也没有做什么出格的事情。[600, 601]

但问题就出在波因德克斯特在给国会提交的报告里举了一个例子，他说这个项目可以用来预测类似“明年恐怖分子是否会用生化武器攻击以色列”这样的事件，而“政策分析市场”网站上用的背景图上竟依稀可以看见“阿拉法特被暗杀”等字样。[602]尽管这个网站到10月才正式启用，但对议员们来说，这已经足够说明问题了，他们立刻集中火力、狂轰滥

炸：让大家打赌猜测恐怖分子想做的事情，实在太荒诞了，资助这样的项目就等于“挥霍纳税人的血汗钱”。[574]

参议院拨款委员会主席西奥多·斯蒂文斯（Theodore Stevens）声色俱厉：“这个项目是国防高新局的一个非常严重的错误。”议员们争先恐后表达愤怒之情。[603]就在新闻发布会的第二天，面对共和、民主两党的高度一致和同仇敌忾，国防部紧急叫停了大家口中的这个“恐怖市场”。[604]其实，“未来预测市场”依据的是“预测市场”理论，这个理论曾经在预测美国总统选举方面取得了很好的应用效果。怀登他们这么说、这么做，主要是利用了项目组的失误、普通美国人的情绪以及其他议员对“预测市场”理论的无知，手段不算高明，但结果出奇好。怀登参议员取得了他进入情报委员会之后的第一次真正胜利。[423]

中国国内学术界在“预测市场”方面发表的学术论文很少。从其运行效果和引起的争议来看，是一个非常有意思的话题，有必要稍微多说几句。“预测市场”理论的灵感来自于经济学家弗里德里希·哈耶克（Friedrich Hayek）的一个假说。哈耶克本人是1974年诺贝尔经济学奖获得者，他认为：价格机制实际上是一种信息交流机制，零散分布的信息可以通过价格机制很好地聚集起来；要采取正确的行动，参与者只需要一点儿信息就够了。[600, 605, 606]

在这一片嘈杂声中，最专业的要数2001年诺贝尔经济学奖获得者约瑟夫·斯蒂格利茨（Joseph Stiglitz）了。他质疑哈耶克的理论过于理想化，“政策分析市场”的理论基础不牢，这个市场预测结果的准确性值得质疑。[607]

波因德克斯特这个时候才意识到当下的情势已经非常危急。他只能使出最后的招数。首先他请老朋友沙基出面，动用他所在的科应公司的游说力量，试图做通国会议员的工作。然后他拐弯抹角找到了国防部前部长佩里，希望他出面挽救自己的“全面信息感知”。佩里还是很给他面子，他找到了掌管国防部“钱袋子”最重要的两个参议员，一个是拨款委员会主席斯蒂文斯，另一个是丹尼尔·井上建（Daniel Inouye）。俗话说“冤家路窄”，井上建参议员正是20年前“伊朗门”特别调查委员会主席。他当年在对波因德克斯特所做的证词中给出了三个评价词：“不可思议、难以置信、令人齿寒”。[598]

终于到了不撤退不足以平民愤的关键时刻。波因德克斯特此时已经

身心俱疲，于是他很快就提出辞职。国会出面否定，国防部壮士断腕，项目停止，信息感知办公室被撤。

回过头看，国防高新局的“全面信息感知”计划惨遭失败，教训有三。

其一，这是由国防高新局固有的运行机制决定的。由他们出面组织研究工作，需要保留一丝信息公开的缝隙：通过在互联网上公开发布待研项目的主要要求，在更大范围内征集更好的研究建议和研究方案，从而确定研究团队。当然，一旦研究团队明确了，后面具体的研究经费、研究进度、研究成果就可以严格保密了。敏感的新闻媒体就是从这一丝丝的缝隙里嗅到了“全面信息感知”计划中蕴含的令人不安的气息，借题发挥、小题大做，最终使得这个计划夭折。相比之下，美国情报圈子里的一些单位早就在开展类似的研究，这些研究项目之所以能够安安稳稳地开展下去，其最大原因是它们秘而不宣，躲开了公众和舆论的视线。

其二，“全面信息感知”计划是明显越界的。虽然反恐战争不仅是军事战，也是情报战，但两者还是有界限的。特别是针对美国国内监视这一块，明确属于联调局和国土安全部的工作范围，由国防高新局主持开展“全面信息感知”计划，等于跑到了这些单位的地界上，本来就欠考虑。

其三，错误地选用波因德克斯特来主持这个计划。从专业方面上讲，他具有很大的优势，既懂技术又懂情报，还懂决策，但他的劣势也很明显——他的负面形象太过深入人心，这导致他一出现，几乎所有的舆论声音都集中在了他身上，而且都不是正面的。

此外，国防高新局拒绝了麦康奈尔的建议，没有事先做通国会议员的工作，获得他们的支持，顽固地相信自己只管技术、不问政治，这也是这个项目失败的重要原因。

就在波因德克斯特最受煎熬的2003年7月，国安局局长第二次向国会的“八人帮”汇报“星风”行动的执行情况。[598]所谓“八人帮”，指的是参众两院的议长和少数党领袖，以及两院情报委员会的主席和副主席。小布什非常清楚，他授权国安局开展的“星风”行动很容易引起争议，于是他借助保密机制，把它列入“特密专案”来限制其知情范围。国会方面则通过“八人帮”机制限制知情范围：只把大致的一些情况告诉这几位重

要人物，并且严格禁止他们对外以及对他们的幕僚和法律顾问透露情况。听完汇报，参议院情报委员会副主席约翰·洛克菲勒（John Rockefeller）提笔给副总统切尼写了一封信，信中写道：

我想就今天讨论的那些敏感的情报问题再次表达我个人的关切。很明显，我们今天讨论的这些工作，在监管方面存在严重的问题……在会上我想到了我们的未来，想到了波因德克斯特的“全面信息感知”计划，不由得更加担心政府处理安全、技术和监视问题的思路和方向。[598]

约翰·洛克菲勒主要是想批评“星风”行动，但他把波因德克斯特和他的“全面信息感知”计划作为一个反面教材，也大抵反映出在议员的心目中波因德克斯特和他的宏伟计划是个什么样子。

从计划曝光开始，大家都已戴上“有色眼镜”，优点被搁在一边、缺点被无限放大。再加上“未来预测市场”这个项目对技术之外的事情考虑不周，成为压垮整个计划的最后一根稻草。

暗度陈仓

“全面信息感知”计划真的就这样完全失败了吗？

在国防部的预算法案里有这样一段：

本法案以及其他法案中所提及的经费拨款，一律不得给予“反恐信息感知”计划（国会拨款委员会不加区别地使用该计划的新名称和原有名称）。[598]

看上去，“全面信息感知”计划真的彻底失败了，给国防部的经费里再没有一分钱会投给这个计划。不过，下面紧接着还有一小段不起眼的说明：

注意：这一限制对于秘密附录中所列举的、已授权的、用于对外反恐情报的处理、分析和协作工具不适用。[598]

其实，国会对“全面信息感知”计划并没有简单地一棍子打死，被严格限制的只是对数据挖掘技术的具体“实施和部署”，对这些技术的研究开发则没有受到任何限制。2003年撤销“全面信息感知”计划和信息感知办公室的时候，国会就和国防部达成了协议，对信息办公室下面的项目进行了分类处理。可惜媒体报道这件事情的时候，没有直接点出具体的项目名称，也就没引起大家的注意。[608]

第一类项目不属于国防高新局的业务范围，因而转入情报部门，准确地说是“国家对外情报计划”（NFIP）的执行单位。这类项目中有一个是在开发“协作式软件，情报人员使用这个软件可以把分散在不同联邦政府单位的情报信息串联起来”，这指的应该是“前帆（二期）”。另外几个项目“借助雷达图像和视频影像中人物的行动特征和面部特征把他们识别出来”，这应该是指“远距人物识别”、“活动–识别–监视”和“下一代人脸识别”这三个项目。[608]

第二类项目属于国防高新局的业务范围，因而转入高新局其他计划办公室继续开展研究，这样的项目有四个，其中两个研究“对抗未来恐怖袭击的兵棋推演”，分别指“非对称环境兵棋推演”和“快速分析型兵棋推

演”这两个项目；另一个研究“加速探测出生物恐怖袭击的方法”，指的是“生物事件首要指标识别技术”项目；还有一个开发“自动翻译外文资料和广播的软件”，是指“多语种语音和文本自动开发”项目。[609]

剩下没有点名的，应该立即停止，例如“预测市场”和“信息感知原型系统”，但实际上未必。

科应公司的全资子公司希克斯伙伴公司在2002年年底得到了“信息感知原型系统”1900万美元的合同。前面说过，这个系统是“全面信息感知”计划的总集成项目，负责把计划研究开发出来的各种信息抽取、分析和分发工具捏成一个拳头、形成一个整体。2003年年末国会撤回了项目资金，按照正常人的想法，公司里这个时候一定是愁云惨雾、哀声一片。沙基——推荐波因德克斯特出山的那位“伯乐”（他除了是科应公司的高管，还是这家希克斯伙伴公司的资深副总裁）在这个节骨眼上，给公司的分包商写了一封电子邮件，主要目的是安抚“军心”、打消顾虑，信中写道：

（国会撤回资金）导致我们的工作在未来存在巨大的不确定性。但幸运的是，我们有了一个新的资助者，它能使我们从前的大部分工作可以继续开展下去。从现在开始，我们把这个新的项目叫作“篮球”。[610]

消息来源确定，这个新的资助者就是国安高新处。

“国防高新局”这个名字跟许许多多获得巨大成功的技术创新关联在一起，如互联网、全球卫星导航系统、隐形飞机。美国国内有一股“向国防高新局学习”的潮流，情报界在这股潮流中更是积极：国安局在1998年成立了“高新研究发展处”（ARDA，简称国安高新处），中情局则建立了“情报技术创新中心”，国家地空情报局下面也设有一个“国家技术联盟”。一句话，这些机构都希望取到国防高新局的“真经”，复制同样的成功与辉煌。

在一份公开的国防部文件中，明确指出“篮球”项目在2004财年得到了全额资助，资助时间一直持续到2004年9月。这份文件说“篮球”系统是一个“闭环的、端对端的早期预警和决策系统原型”，这和2002年希克斯伙伴公司签订的“信息感知原型系统”合同上的说法完全一致。[610]这也印证了“篮球”系统就是“信息感知原型系统”。文件还说，国安高新处和科应公司联办的一个研究中心已经完成了系统测试。

“全面信息感知”计划中的“前帆（二期）”项目也被悄悄转入国安高新处。“马甲”是必须要换的，新的“马甲”叫“顶帆”（TOPSAIL）。就在2005年10月，科应公司还得到了“顶帆”项目370万美元的合同。官方发布的项目材料说，“顶帆”的目的是为情报分析人员和决策人员团队提供支撑工具，帮助他们预测和阻止恐怖袭击。这些话和当初“前帆（二期）”的合同文本、预算文件以及项目经理的发言材料几乎一模一样。[610]

除了这些研发项目，波因德克斯特还在“全面信息感知”计划中建立了一个演示验证各种研发成果的试验网络。试验网络所需要的设施国防高新局里可没有。特瑟局长给他出了一个主意，可以利用陆军情报与安全司令部的场地和设施，这个单位位于弗吉尼亚州的贝尔沃堡，司令和波因德克斯特一样，是一位“极客”。[578]

他就是后来的国安局局长亚历山大。

亚历山大来自海军研究生院，手里握有两张硕士文凭，一张是电子战专业的，另一张则属于物理学专业。这位在雪城城郊长大的少年先是考入西点军校，毕业后不停地从国安局的一个基地跳到另外一个基地。2001年，亚历山大被任命为陆军情报与安全司令部司令，肩上有了一颗将星。“9·11”事件之后，他命令陆军情报人员非法监视普通美国人的电话和电子邮件，种种表现深得国防部部长拉姆斯菲尔德赏识。[344]

波因德克斯特早就认识此人。若干年前亚历山大曾经参与过“前帆”项目的演示验证工作。在得知波因德克斯特的请求后，亚历山大司令很痛快地就答应了下来。他告诉波因德克斯特，他们可以使用他在信息控制中心（IDC）的场地，以及现成的网络设施。并且，司令还很“慷慨”地把秘密搜集的数据与其共享，“全面信息感知”计划开发出来的各种工具可以利用这些实际数据进行测试。波因德克斯特立刻就决定把试验网络中心放在这里。[578]

信息控制中心在情报圈子里非常有名。因为它是模仿《星际迷航》里“企业号”飞船的驾驶舱来装修房间，有金属的台面，巨大的显示墙，就连开关门的声音也和影片里一样。在这部包括了若干部电视剧、动画片和电影素材的影视作品里，男主角名叫“寇克”，于是，许多人把信息控制中心大厅中央的那把不锈钢座椅称作“寇克舰长的椅子”。在建设之初，军方还特地咨询了迪士尼公司的设计师。由于这种风格和亚历山大

司令的气质吻合，所以经常有人以为这是他主持修建的，不过实际情况是，中心修成这样和亚历山大并没有关系。[611, 612]

尽管“全面信息感知”计划已经下马，波因德克斯特建立的试验网络却并没有受到影响，只是改名为“研究开发试验协作”网络（RDEC）。试验照常进行，网络规模还在稳步扩大。就在波因德克斯特辞职的当月，一场代号“沙其风”（SHARQI）的试验在这里进行得如火如荼。到2003年年底，这个试验网络的单位节点超过了27个，个人用户超过350人。[613]

负责接手“全面信息感知”计划的国安高新处总共只有8个正式员工，这个单位并没有出现在政府机构黄页上[614]，他们的网站早已不复存在，仿佛围绕这个单位的所有事情都从未发生过一样。但高新处的工作可不只是接收从“全面信息感知”计划转移过来的项目，他们有自己的高新技术研究计划，每年的经费预算大概1亿美元。“9·11”事件之前高新处主要关注图像识别技术，特别是人脸识别技术，2000年他们资助了9家单位开展这方面的研究工作。“9·11”事件之后，他们启动了一个名字很漂亮的研究计划，叫作“海挖”（NIMD，海量数据挖掘新颖情报）。[615]有“好事者”对高新处的部分网站内容做了存档，从这些存档材料里还可以看到高新处以及“海挖”计划当年的模样。

美国情报界的中心任务是帮助国家避免遭受战略突袭。我们所说的“战略突袭”是事先未预料到的国家安全重大事件——这些事件将引起国家级的反应。“9·11”事件就是这样的例子……从规模、类型和复杂度不断增大增多的数据中发现突袭迹象、预测突袭发生，这是情报分析人员的责任。[616]

今天看来，这简直就是美国情报界的大数据宣言。

“海挖”计划的目的是帮助分析人员把注意力放在海量数据中最重要的信息上——这些信息能把潜藏的战略突袭揭示出来。

“新颖情报”，是从前未被分析人员和决策者掌握的、具有可操作性的信息，它能帮助分析人员洞悉之前未被注意或者未被理解的种种威胁。海量数据带来的问题源自多个方面：对分析深度而言，数据规模可能是个问题；对分析广度而言，数据异构可能是个问题；当然，数据的复杂性本身就是个问题。

仅仅是大量的相似数据，比如达到拍字节以上规模，就可以叫作“海量”数据。某些类型的情报数据源每个月的数据量就能达到4拍字节，并且还在加速增长。

另外一些数据，尽管规模不那么大，但其中包含许许多多类型和格式各不相同的信息对象，也被认为是“海量”……

还有一类数据，它们内在的复杂性很强，比如每个文档都包含了多个信息对象，并且这些对象之间互相关联，也就是说每个信息对象的意义都取决于其他对象包含的信息，这样的数据也会被认为是“海量”。要理解这些复杂数据的内容，需要具备处理融合数据的能力，这超出了当前的技术范围。更深层次的复杂性问题是由于某些数据处于不同领域的交汇点上，要全面理解这些信息，需要多方面的经验。例如，对于某个事件或某个地点，分析人员可能需要考虑有关它们的社会、军事、经济、政治、政府、科技等方方面面的问题。[616]

即使放到今天来看，这份宣言里对三种类型海量数据的描述，仍然可以看作对“大数据”的一种非常准确、非常清晰的界定。

2004年的一天，重新回归宁静的波因德克斯特手边的电话突然响了起来。电话另一头是老朋友理查德·珀尔（Richard Perle）。当年波氏担任里根总统国家安全事务助理的时候，珀尔是国防部负责全球战略的助理部长。珀尔问他，愿不愿意到自己家来一趟，见一见两位来自硅谷的企业家，一位名叫彼得·泰尔（Peter Thiel），另一位叫亚历克斯·卡普（Alex Karp）。泰尔的故事很多，他是商业圈里非常有名的风险投资人，眼光独到，他看准的互联网公司中有很多后来都成为业内骄子，比如提供在线支付服务的贝宝公司、稳坐社交网络第一把交椅的脸谱公司。而这一天，他的身份是刚建立不久的帕兰特公司的联合创始人，和他在一起的卡普也是这家公司的创始人，当时还是公司的首席执行官。[617]

在线支付的核心是建立一套信用系统，通过分析交易数据，把各种可疑的、欺诈的模式发掘出来，使顾客免受损失。泰尔认为贝宝防止信用诈骗的核心算法，可以用到预防恐怖袭击和犯罪这件事情上，其背后蕴含着无限商机，于是和其他几个人一起，创立了这家新公司——帕兰特。他们的这种想法和波因德克斯特主持的“全面信息感知”计划中广泛涉及的“数据挖掘”颇有几分神似。波因德克斯特后来回忆说：“我告诉他

们，我认为他们的点子很有意思。”他还说，他们拿出来的试验产品的用户界面“绝对漂亮”。[617]

除了波因德克斯特，泰尔和卡普在那段时间请教过的“专家”还有“灌篮”总监特内特，他从总监的位置上退下来后还被这家公司聘为顾问。截至2005年，帕兰特公司的主要经济来源和唯一顾客只有泰尔的贝宝，直到公司从中情局下属的风险投资机构“因奎泰尔”那里得到了200万美元的资金投入，公司才算真正起飞。随后三年，中情局成为帕兰特公司最主要的投资人和顾客。公司在为中情局“服务”的过程中，可以接触到局里的各种秘密数据库和大量富有经验的专家，也逐步积累了一大批将来可用的政府客户，这才是对帕兰特日后发展更重要的一件事情。[618]鲍顿在他的《大结局：击毙本·拉登》（*The Finish: The Killing of Osama Bin Laden*）一书中隐晦地透露，有关本·拉登的线索所涉数据纷繁复杂、数量巨大，帕兰特公司的软件产品可能用于对这些数据的分析工作，是名副其实的“杀手级应用”。[619]这样一种说法，随后借《福布斯》杂志之口，以该公司“据传帮助追杀本·拉登”的语气传遍天下。[620]是真是假，无法深究。确凿无疑的一点是，这家主要面向国安局、中情局、联调局以及花旗银行等客户的新兴公司，成立不过10年，到2014年年底，市值就超过了90亿美元，在大数据分析方面已经可以和IBM、博艾汉这样的老牌公司一争高下了。[621]

2005年，大规模杀伤性武器情报反思报告发布。报告提出，赋予国家情报总监更实在的权力，以便其更好地发挥协调、组织美国情报界各单位开展工作的职能。这条建议很快就开始得到落实。高新技术研究方面统一协调力量相对容易一些，于是先把国安局的国安高新处拿了过来，放在国家情报总监办公室之下，改名为颠覆性技术办公室（DTO），再把这个办公室与地空情报局的国家技术联盟、中情局的情报技术创新中心合并（还有一种说法，颠覆性技术办公室与其他两家单位合并之前，仍属于国安局[622]），打造成美国情报技术研发的“国家队”——情报高新局。新成立的单位没有地方办公，一番论证之后，情报总监办公室决定，新建一栋现代化的办公大楼，可是“远水解不了近渴”，新大楼估计要几年后才能盖好，情报高新局的办公场所问题必须立刻解决。他们想起了马里兰大学语言高级研究中心这块“宝地”，于是和学校商量妥当了借用事宜。不久，情报高新局就搬进了马里兰大学语言高级研究中心[623]。

就在几个月前，年轻的斯诺登刚刚结束了他的第一份正式工作，离开了这里。

尾声

2013年7月2日，玻利维亚总统埃沃·莫拉莱斯（Evo Morales）参加完在俄罗斯召开的天然气输出国峰会，乘坐专机启程回国。但是法国、意大利、葡萄牙和西班牙四国先后发来通知，要么是不允许总统的飞机通过他们的空域，要么是拒绝这架飞机在他们的机场着陆。[624]最终，专机只能在奥地利迫降。后来人们才知道，之所以发生这一切，是因为美国的情报单位报告白宫，斯诺登很可能在这架飞机上。于是美国政府给有关国家打了招呼，威胁说“如果让斯诺登进入他们的领土将会严重损害他们与美国的关系”[625]，这样便硬是把莫拉莱斯的飞机截留在了维也纳。

但是，让美国人颜面尽失的是，他们让奥地利人把这架飞机里里外外搜了一遍，却没能找到斯诺登的踪影。[624]等到飞机再次起飞，莫拉莱斯总统在机场已经滞留了12个小时。[626]总统本来就十分懊恼，前来看望他的奥地利副首相竟然还对记者说他是“自愿接受检查”，奥地利人是“在玻方的邀请下”登上飞机检查每件东西的。[625]除了生气，莫拉莱斯也只能生气，无可奈何。

美国国家安全委员会的发言人凯特琳·海顿终于发声，这是官方对此事的正式说法：

美国并没有要求任何一个国家强行拦下莫拉莱斯总统的飞机。我们做的……只是通过外交和正当法律渠道，同斯诺登可能过境的那些国家联系了一下。[627]

“联系了一下”，意味着美国仅仅显露了一下舌尖上的、指尖上的肌肉，轻轻松松就迫使一个国家的元首“自愿接受检查”。阿根廷总统发表评论说，这一事件含有“我们本以为被彻底消灭了的殖民主义的残余”，是羞辱了整个南美洲的行径。厄瓜多尔总统也表示，这是对整个拉丁美洲的辱没。[628]

此时此刻，斯诺登已经在莫斯科谢列梅捷沃国际机场滞留了9天。从他被困在机场过境区的第一天起，来自美国国务院、中情局、联调局等政府部门的高级官员几乎每天都要到白宫开会，苦思冥想如何把斯诺

登捉拿归案。国土安全事务助理说："对我们来说最好的情况是他在第三国着陆。我们都希望他会特别愚蠢地登上某架飞机，然后我们的盟友说：'这是我们的飞机！立刻着陆！'"[627]这是一种多么可笑的想法！正是因为他们低估了斯诺登的机警，才发生了莫拉莱斯总统飞机迫降事件。事实证明，这些高级官员的想法只能是痴人说梦，不会有一点点实现的可能。8月1日，斯诺登在到达俄罗斯39天之后，终于走出机场——俄罗斯政府给了他为期一年的临时庇护。

7月10日，著名的黑客大会"Defcon"宣布，由于发生了"斯诺登事件"，大会不再欢迎联邦政府官员参加他们的活动。就在一年前，亚历山大局长还以一袭黑色T恤亮相，一副轻松的样子在会上侃侃而谈。他说："有传言说我们建立了成百上千万民众的档案，那是绝对错误的。"[629, 630]可惜那铿锵的话音还在耳边，现在已经曝光了相关档案材料，局长显得如此尴尬。好在，另一个黑客大会"黑帽子"继续邀请局长到会讲话，算是替他挽回了一点儿面子。亚历山大这一回一身军装、一脸严肃。上次他主要是想规劝黑客们为美国政府效劳，这次则主要是来替美国政府的监视行动辩护，效果如何，自不必说。[631]

半个月后，在阿斯彭举办的安全论坛上，国安局正式确认，针对"斯诺登事件"暴露出来的安全隐患，国安局出台了一系列新的规定，第一条就是类似于操作核武器的"双人规则"，即如果系统里有高度机密的资料，则需要两名系统管理员同时操作。亚历山大局长说，国安局正在计划把最敏感的数据以高度加密的形式保存，同时严格控制系统管理员的人数，就因为斯诺登曾经担任过系统管理员，有权力在情报单位和国防部系统中把数据移来移去。局长承认："这将使我们的工作更为困难。"[454]

8月9日，奥巴马总统首次就各种监视行动正式表态，他提出要提高情报机构的透明度，却并没有宣布采取任何措施来向民众公开监视行为。他还提出建立一个专门小组审查情报政策。这个专门小组的名字听上去有些做作而可笑——"情报和通信技术审查小组"。从一开始，批评人士就把这个小组称为白宫的傀儡。[502]几个月后，这个小组还真的提出了一些意见。比如，他们建议把赛博司令部从国安局中分离出来。这条意见遭到了麦康奈尔、海顿和亚历山大等人的一致反对，被奥巴马舍弃。又比如，他们建议在电话监视行动中，国安局不再保存数据记录，改由通信公司或者第三方保存。这条意见遭到通信公司的强烈反

对。[632]总而言之，他们提出的这些意见或者是纸上谈兵、不接地气，或者只是虚晃一枪、做做样子。

10月的最后一天，格林沃德在《卫报》网站上刊登了一篇离别感言，宣布自己正式离开《卫报》。引人注意的是，他不仅留下了电子邮箱，还留下了自己的PGP公钥。在“易趣网”老板的资助下，格林沃德和波伊特拉斯等人成立了一家新的独立媒体，他们以这个名为“拦截”的电子杂志为阵地，继续发表文章揭露各种黑幕。半年后，《卫报》美国分社和《华盛顿邮报》因为报道美国国安局的大规模情报监视活动，荣获2014年度普利策奖，格林沃德、波伊特拉斯、麦卡斯基尔和戈尔曼等人分享了这一荣誉。当然，没有人会忘记斯诺登。《纽约客》杂志专门刊发文章，标题就是“斯诺登的普利策”。波伊特拉斯说：斯诺登想让大众知道美国政府正在干什么，获此殊荣就是对他的勇气和渴望的完美辩护。[633]斯诺登也发表了热情洋溢的声明，对记者们的辛勤付出表示诚挚的感谢。他说：“他们的工作将为我们创造更加美好的未来”。[634]

荣誉背后，甘苦自知。吉布森就说，2013年的这些报道工作“紧张激烈、让人殚精竭虑，有时甚至胆战心惊”。[633]好在，她的付出得到了回报。曾经担任《卫报》美国分社主编的她已经从纽约回到伦敦，升任总社网络版总编。[635]同在纽约的另一位女强人、《纽约时报》总编艾布拉姆森则卷入报社的一次内讧，随后黯然退场。[636]她从拉斯布里奇手里拿到斯诺登的文件后虽然也组织了一些报道，但最佳时机已经错过，最终没能超过《卫报》和《华盛顿邮报》引起的反响。这可能才是报社上层对她不满意的深层次原因。

2014年1月23日，“隐私与民权监督委员会”（PCLOB）发布了第一份有关美国情报单位开展大规模监视行动的报告，报告指出，依据《美国爱国者法案》第215条开展的电话记录搜集计划缺少确凿的法律依据，导致公众对宪法第一和第四修正案忧心忡忡，此举对隐私和民权构成严重威胁，并且计划的实际价值不大。“因此，该委员会建议政府终止这一计划。”[637]

这个委员会是根据“9·11”事件委员会的建议在2004年设立的，原本隶属于白宫。不过设立之后很多年都“趴”着没动，2007年国会决定将其改制为一家独立机构，同时授予其接触各种密级计划的权力，但这个委员会仍然没有开展工作——因为人员没有配齐，直到2011年年底奥巴马总统才算解决了人员问题，但其实说起来总共也就5个人。[441]

很多人都期待委员会接下来拿出的报告也同样有力，果真如此的话，推进美国情报机构调整和整顿的可能性就会很大，从根本上解决大规模监视问题的可能性也会很大。但是，7月初报告出炉，力主改革的这些人便泄气了。报告指出，依据《外国情报监视法案》（修正案）第702条开展的监视计划“合法且有效”，当然也存在一些个人隐私的问题。[638]“考虑到恐怖主义，涉及美国国内某些人的通信数据是通过这个（监视）计划搜集到的通信数据中最重要的一部分。”[639]换句话说，“棱镜”计划、“上游”四计划，以及许许多多被揭露和没有揭露出来的计划还应该继续下去。所以，新上任的国安局局长、海军上将迈克尔·罗杰斯（Michael　Rogers）就说，尽管斯诺登给国安局的工作带来了很多挫折，但他不会哀叹“噢，上帝，天塌下来了”。[640]的确，国安局的天没有塌下来，一切还将继续。

对了，被斯诺登弄得有点儿灰头土脸的亚历山大局长正式退休了，成为到目前为止在任时间最长的一位国安局局长。据他自己说，多年以前他就准备退休了，因为一任国安局局长的任期也就是三四年。2009年夏，国防部长给他打电话说：“别那么着急。我们这里还有很多事情需要你做，我们想把你的任期延长到2012或者2013年。”2012年，他又接到新一任国防部部长和参联会主席的电话，依然是挽留，这次的说法是他可以继续做到2014年春天。[565]

由于斯诺登的“功劳”，最近一次对话变成了这样：

“谁应该对此负责？”

“我。这是我的部门，我是局长，最终应该由我来负责。如果每个人都在考虑应该有人对此负责，那就应该是我。其他人做的都是我命令他们做的。如果你要开除谁的话，那就开除我吧。”[565]

亚历山大局长暗自在心里把斯诺登犯下的“罪行”一笔一笔都烙了下来：

32次泄露美国秘密情报工具和方法。

9次泄露美国海外情报基地位置。

25次泄露美国情报单位关注的外国官员、政府和能力。

14次泄露协助美国情报活动的公司和政府信息。

19次泄露美国国安局正在研发的技术产品和技术平台信息。[565]

也由于斯诺登的“功劳”，亚历山大几乎成为国安局历史上曝光率最高的一位局长。即使卸下局长的重任，他的上镜率仍然很高。刚一退休，他就和别人一起创建了一个叫作“铁网赛博安全”的公司，继续发挥“余热”，月薪为60万～100万美元。这样的收入水平高得惊人。他说自己拿高薪靠的是他发明的专利技术，可以检测到恶意的黑客以及赛博入侵者。可是薪酬如此之高自然也就免不了有人在背后指指点点，说他申请了与先前的职务直接相关的专利，这在退休下来的国安局局长里算是首例。[641]

除此之外，亚历山大还做了一件出人意料的事情。他和国安局现任首席技术官帕特里克·多得（Patrick Dowd）签了一份秘密协议，多得每周在他的公司里工作20个小时，其余时间则在国安局上班。这样一份荒唐的协议，国安局的有关部门竟然批准了。[642]美国政府公职人员尽管可以“旋转”到私营部门，但其间有一个“冷冻期”的最低门槛需要跨越，同时在政府和私营单位兼职是不允许的。亚历山大、多得以及国安局做的这件事情也算创造了美国“旋转门”的一个新纪录。

接替亚历山大的罗杰斯很早以前就被看作下一任局长的不二之选。[643]曾有人问起罗杰斯对斯诺登的看法，他回答：“斯诺登不大可能是外国特务，他很相信他所做的事情，我却很怀疑，我和他看法不同。我根本不认同他做的这些事情。我相信那是错的、非法的。”[644]

2014年11月18日，尽管多数参议员支持，但旨在结束美国国内大规模监视活动的《美国自由法案》以两票之差未能在参议院通过。不过，法案的发起者宣布他们不会放弃战斗。[645]

斯诺登的律师宣布，俄罗斯政府决定把斯诺登的庇护期延长至2017年。据律师说，斯诺登已经在当地找到了一份工作，靠工资和捐款生活。[646]他的女朋友米尔斯也来到俄罗斯，和他生活在一起。

波伊特拉斯以她在香港采访斯诺登的经历为基础，创作了一部纪录片——《第四公民》（*Citizenfour*）。片名是斯诺登第一次和波伊特拉斯联系时使用的别名，主人公当然是他。这部电影为波伊特拉斯赢得了她的第一座奥斯卡小金人。和她一同参加颁奖仪式的有格林沃德，还有

斯诺登的女朋友米尔斯。[647]斯诺登本人因为显而易见的原因未能出席。

在这部影片里有一个镜头，斯诺登在莫斯科见到了格林沃德，记者说出来的信息让他大吃一惊：除了他之外，格林沃德还在跟另外一个情报源联系。而较早之前，美国有线新闻网就曾经推断，除了斯诺登之外，至少还有一个人在泄露国安局的秘密。因为有一份披露出来的材料显示的时间是在斯诺登开始逃亡之后。[648]班福德在不同的地方接触过斯诺登文件的完整拷贝，他发现，有若干份披露出来的材料，在这些拷贝中根本找不到。于是他推断，在某个地方一定还有另外一个正泄露国安局秘密的人。[15]

那么他会是谁呢？他又在哪里呢？

缩略语对照表

AAD：Advanced Analysis Division；（美国国家安全局）先进分析处

AFSA：Armed Forces Security Agency；（美国）武装力量安全局

AINTA：Army INTelligence Agency；（美国）陆军情报局

AINTC：Army INTelligence Command；（美国）陆军情报司令部

ANT：Advanced Network Technology，或Access Network Technology；（美国国家安全局）先进网络技术科，或网络访问技术科

ARDA：Advanced Research and Development Activity；（美国国家安全局）高新研究发展处，简称国安高新处

ASA：Army Security Agency；（美国）陆军安全局

ATO：Access Technologies Operations Branch；（美国国家安全局）获取技术行动科

AUMF：Authorization for Use of Military Force；（美国）使用军事力量授权法

BCT：Brigade Combat Team；旅战斗队

BRUSA：Britain–United States of America agreement；不列颠与美国通信情报协议

BSA：Bank Secrecy Act；（美国）银行保密法案

C4ISR：Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance；指挥、控制、通信、计算机、情报、侦察和监视

CASL：Center for Advanced Study of Language；（美国马里兰大学）语言高级研究中心

CDAA：Circularly Disposed Antenna Array；环形配置天线阵

CEO：Chief Executive Officer；首席执行官

CIA：Central Intelligence Agency；（美国）中央情报局，简称中情局

CNE：Computer Network Exploitation；计算机网络开发

CNI：Classified National Intelligence；（美国）涉密国家情报

COMINT：COMmunications INTelligence；通信情报

CONUS：the CONtinental United States；美国本土

CRS：Congressional Research Service；（美国）国会研究部

CSC：Computer Sciences Corporation；计算机科学公司，简称计科公司

CSS：Central Security Service；（美国）中央安全局，简称中安局

CSSG：Communications Systems Support Group；（美国国家安全局）通信系统支持处，是特搜部（SCS）的掩护名称

DCIA：Director of the Central Intelligence Agency；（美国）中情局局长

DARPA：Defense Advanced Research Projects Agency；（美国）国防高新研究计划局，简称国防高新局

DCI：Director of Central Intelligence；（美国）中央情报总监

DERA：Defence Evaluation and Research Agency；（英国）国防评估研究局

DES：Data Encryption Standard；数据加密标准

DHS：The Department of Homeland Security；（美国）国土安全部

DITU：Data Intercept Technology Unit；（美国联邦调查局）数据侦听技术部

DNI：Digital Network Intelligence；数字网络情报，互联网数据

DNI：Director of National Intelligence；（美国）国家情报总监

DNT：Data Network Technologies Branch；（美国国家安全局）数据网络技术科

DoD：Department of Defense；（美国）国防部

DoJ：Department of Justice；（美国）司法部

DSB：Defence Security Branch；（澳大利亚）国防安全处

DSTL：Defence Science Technology Laboratory；（英国）国防科学技术实验室

DTO：Disruptive Technology Office；（美国国家情报总监办公室）颠覆性技术办公室

DTS：Diplomatic Telecommunications Service；（美国国务院）外交通信处

ECPA：Electronic Communications Privacy Act；（美国）电子通信隐私法

ECSU：Electronics and Communication Surveillance Unit；（美国联邦调查局）电子通信监视部

EO：Executive Order；（美国）总统令

FAA：FISA Amendments Act；（美国）外国情报监视法案修正案

FBI：Federal Bureau of Investigation；（美国）联邦调查局，简称联调局

FISA：Foreign Intelligence Surveillance Act；（美国）外国情报监视法案

FISC：Foreign Intelligence Surveillance Court；（美国）外国情报监视法庭

FLAG：Fibre optic Link Around the Globe；环球光纤链路

FOUO：For Official Use Only；（信息）限官方使用

GAO：Government Accountability Office；（美国国会）政府调查办公室

GC&CS：Government Code and Cypher School，（英国）政府密码学校

GCHQ：Government Communications Headquarters；（英国）政府通讯总局，简称政通局

GED：General Educational Development；（美国）普通教育发展（文凭）

IAEA：International Atomic Energy Agency；国际原子能机构

IAO：Information Awareness Office；（美国国防高新局）信息感知办公室

IARPA：Intelligence Advanced Research Projects Agency；（美国）情报高新研究计划局，简称情报高新局

IC：Intelligence Community；（美国）情报圈子，情报界

ICA：Intelligence Community Assessment；（美国）情报界评估报告

ICP：Internet Content Provider；互联网内容提供商

IDA：Institute for Defense Analyses；国防分析研究所

IMEI：International Mobile Equipment Identity；移动设备国际识别码

IMSI：International Mobile Subscriber Identity；移动用户国际识

别码

INA：Immigration and Nationality Act；（美国）移民与国籍法案

INSA：Intelligence and National Security Association；情报及国家安全协会

INSCOM：INtelligence and Security COMmand；（美国陆军）情报安全司令部

IPSec：Internet Protocol Security；互联网协议安全（协议）

ISA：Intelligence Services Act；（英国）情报工作法案

ISG：Iraq Survey Group；伊拉克（大规模杀伤性武器）核查组

ISP：Internet Service Provider；互联网服务提供商

ITT：International Telephone and Telegraph；国际电话电报公司，简称国电公司

LBO：Leveraged Buyout；杠杆收购

MAC：Media Access Control；媒体访问控制（地址），或硬件（地址）

MCOC：Misawa Cryptological Operations Center；（美国中央安全局）三泽密码行动中心

MCT：Multiple Communications Transaction；多次通信事务

MDR：Massive Data Repository，或Mission Data Repository；海量数据仓储，或任务数据仓储

MIP：Military Intelligence Program；（美国）军事情报计划

MIT：Mission Infrastructure Technologies Branch；（美国国家安全局）任务基础架构技术科

MLCA：Money Laundering Control Act；（美国）洗钱控制法案

MSNBC：MicroSoft National Broadcasting Company；微软国家广播公司

MSOC：Misawa Security Operations Center；（美国中央安全局）三泽安全行动中心

MVR：Massive Volume Reduction；海量数据规模缩减

NAS：National Academy of Sciences；（美国）国家科学院

NCTC：National Counterterrorism Center；（美国）国家反恐中心

NFIP：National Foreign Intelligence Program；（美国）国家对外情报计划

NGA：National Geospatial-Intelligence Agency；（美国）国家地理空间情报局，简称地空情报局

NIE：National Intelligence Estimate；（美国）国家情报评估报告

NIETP：The National Information Assurance Education and Training Program；（美国国家安全局）国家信息保障教育培训计划

NIMD：Novel Intelligence from Massive Data；海量数据挖掘新颖情报（计划），简称海挖

NIP：National Intelligence Program；（美国）国家情报计划

NME：National Military Establishment；（美国）国家军事部

NRO：National Reconnaissance Office；（美国）国家侦察局

NSA：National Security Agency；（美国）国家安全局，简称国安局

NSRL：National Signals intelligence Requirements List；（美国）国家信号情报需求清单

ODNI：Office of the Director of National Intelligence；（美国）

国家情报总监办公室

OEO：Office of Economic Opportunity；（美国）经济机会办公室

OIPR：Office of Intelligence Policy Review；（美国司法部）情报政策审核办公室

OLC：Office of Legal Counsel；（美国司法部）法务办公室

OMB：Office of Management and Budget；（美国）行政管理与预算办公室

OPC-1：Overseas Processing Centre 1；（英国政府通讯总局）海外情报处理一号中心

OTR：Off-The-Record；无痕迹（聊天软件）

PAA：Protect America Act；（美国）保护美国法案

PCLOB：Privacy and Civil Liberties Oversight Board；隐私与民权监督委员会

PDB：The President’s Daily Brief；总统每日简报

PGP：Pretty Good Privacy；超好隐私（加密软件）

PPTP：Point-to-Point Tunneling Protocol；点对点隧道协议

PSP：President’s Surveillance Program；总统监视计划

RCA：Radio Corporation of America；美国无线电公司，简称美电公司

RDEC：Research Development and Experimental Collaboration；研究开发试验协作（网络）

RIPA：Regulation of Investigatory Powers Act；（英国）调查权力法案

RSOC：Regional Security Operations Center；（美国中央安全局）区域安全行动中心

SAIC：Science Applications International Corporation；科学应用国际公司，简称科应公司

SARC：Signals Intelligence Automation Research Center；（美国国家安全局）信号情报自动化研究中心

SBU：Sensitive But Unclassified；（信息）敏感但非密

SCI：Sensitive Compartmented Information；特密信息，敏感隔离信息

SCS：Special Collection Service；（美国国家安全局）特殊搜集部，简称特搜部

SID：Signals Intelligence Directorate；（美国国家安全局）信号情报分局

SIGAD：SIGINT Activity Designator；（美国国家安全局）信号情报行动编号

SSA：Signal Security Agency；（美国陆军）信号安全局

SSBI：Single Scope Background Investigation；单一范围背景审查

SSE：Special Source Exploitation；特殊情报源开发

SSL：Secure Socket Layer；安全套接层（协议）

SSO：Special Source Operations；（美国国家安全局）特殊情报源行动处，简称特情处

SSSS：Secondary Security Screening Selection；二级安全筛查对象

TAO：Tailored Access Operations；（美国国家安全局）特别接入行动处，简称特接处

TDY：Temporary DutY；临时任务

TIA：Total Information Awareness，或Terrorism Information

Awareness；全部信息感知（项目），或反恐信息感知（项目）

TNT：Telecommunications Network Technologies Branch；（美国国家安全局）通信网络技术科

TOR：The Onion Router；洋葱头（路由软件）

TSP：Terrorists Surveillance Program；反恐监视计划

UCLA：University of California, Los Angeles；加州大学洛杉矶分校

UKUSA：United Kingdom – United States of America Agreement；联合王国与美国通信情报协议

UNESCO：UN Educational, Scientific & Cultural Organization；联合国教科文组织

USC：United States Code；美国法典

UTT：Unified Targeting Tool；目标锁定一体化工具

VHF：Very High Frequency；（信号）甚高频

VLF：Very Low Frequency；（信号）甚低频

WMD：Weapon of Massive Destruction；大规模杀伤性武器

参考文献

[1] ANDREW CARD[J/OL].[2014-01-05]http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-andrew-card/.

[2] MCQUILLAN L.White House to move to Texas for a while[N].USA TODAY, 2001-08-03.

[3] DAN BALZ B W.America's chaotic road to war[N].The Washington Post, 2002-01-27.

[4] GEORGE TENET B H.Shot out of a cannon[M].At the center of the storm: The CIA during America's time of crisis.New York: Harper Perennial, 2008.

[5] GEORGE TENET B H.9/11[M].At the center of the storm: The CIA during America's time of crisis.New York: Harper Perennial, 2008.

[6] WOODWARD B.Two months before 9/11, an urgent warning to rice[N].The Washington Post, 2006-10-01.

[7] WINDREM R.Evidence piles up that Bush administration got many pre-9/11 warnings[J/OL].[2012-09-11]http://investigations.nbcnews.com/_news/2012/09/11/13809524-evidence-piles-up-that-bush-administration-got-many-pre-911-warnings.

[8] 康多莉扎·赖斯.无上荣耀[M].长沙：湖南人民出版社，2014.

[9] KAPLAN F.The Out-of-Towner[M].Slate, 2004.

[10] PARRY R.The real lessons of 9/11[M].Baltimore chronicle.The Baltimore News Network, 2009.

[11] THOMAS DRAKE[J/OL].[2013-12-10]http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/.

[12] WILLIAM BINNEY[J/OL].[2013-12-13]http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-william-binney/.

[13] MICHAEL HAYDEN[J/OL].[2014-01-02]http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-michael-hayden/.

[14] SHANA LYNCH.Former NSA Head Michael Hayden: The agency “cannot survive without being more transparent”[M].Stanford Business, 2014.

[15] BAMFORD J.Edward Snowden: The untold story[M].Wired, 2014.

[16] 乔治·沃克·布什.抉择时刻[M].北京：中信出版社，2011.

[17] 乔治·沃克·布什.抉择时刻[M].北京：中信出版社，2011.

[18] JR.R O H.Six weeks in autumn[M].No place to hide.Free Press，2006.

[19] 钱昌明.普京铁拳惩“俄奸”：有感于俄罗斯版“爱国者法案”的出台[EB/OL].[2014-05-09] http: //bbs1.people.com.cn/post/1/1/2/139201425.html?from＝singlemessage & isappinstalled＝0.

[20] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) ACT[M].2001.

[21] 刘卫东.《美国爱国者法》及其对美国公民权利的影响[J].美国研究, 2006, 1.

[22] ELLIOTT J.Patriot Act critics never had a clue[M].Salon, 2013.

[23] DREHER C.He knows what you’ve been checking out[M].Salon, 2002.

[24] FEINGOLD R.On voting against the U.S.A.Patriot Act[J].Archipelago, 2002, 6(2).

[25] DANA PRIEST W M A.Top secret America: Part 1: A hidden world, growing beyond control[N].The Washington Post, 2010-07-19.

[26] GOOD D.Bill Clinton, hours before 9/11 Attacks: ‘I could have killed’ Osama bin Laden[J/OL].[2014-08-01]http://abcnews.go.com/US/bill-clinton-hours-911-attacks-killed-osama-bin/story?id＝24801422.

[27] 乔治·沃克·布什.抉择时刻[M].北京：中信出版社，2011.

[28] Address to a Joint Session of Congress and the American people[J/OL].[2001-09-20] http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html.

[29] JOEL DYER D A, JEFFERSON DODGE.NSA uses ‘terrorism’ to justify mass surveillance that started long before 9/11 and the Patriot Act[N].Boulder Weekly, 2013-06-20.

[30] NUGENT T.Inside the 9/11 Commission[M].@UCSD magazine, 2005.

[31] 赵秉志，王志祥，王文华等.“9·11”委员会报告：美国遭受恐怖袭击国家委员会最终报告[M].北京：中国人民公安大学出版社，2004.

[32] The 9/11 Commission Report[M].2004.

[33] 黄乐平，蔡永强，张龙秋.揭秘9/11：美国遭受恐怖袭击国家委员会最后报告[M].北京：中央编译出版社，2005.

[34] 戴维·罗特科普夫.美国国家安全委员会内幕[M].北京：商务出版社，2013.

[35] Ivins case reignites debate on anthrax[N].The Baltimore Sun, 2008-08-03.

[36] BHATTACHARJEE Y.FBI to request scientific review of its

anthrax investigation[M].Science Now, 2008.

[37] DAVID A.KAY: America's weapons sleuth talks about his experiences searching for Iraq's weapons of mass destruction[M].Chemical & Engineering News.American Chemical Society, 2004.

[38] ELBARADEI M.Iraq, 2002 and after: a needless war[M].The age of deception: nuclear diplomacy in treacherous times.Picador, 2012.

[39] Iraq's continuing programs for weapons of mass destruction[M].2002.

[40] LEIBOVICH M.George Tenet's 'Slam-Dunk' into the history books[N].The Washington Post, 2004-06-04.

[41] WOODWARD B.Plan of attack[M].New York: Simon & Schuster, 2004.

[42] JR.R A B.Leadership of the U.S.Intelligence Community: From DCI to DNI[J].International Journal of Intelligence and CounterIntelligence, 2014, 27(2).

[43] LINZER D.Goss, 8 Ex-Chiefs of CIA mark old post's passing[N].The Washington Post, 2005-08-17.

[44] 国际原子能机构总干事穆罕默德·巴拉迪先生在安理会上的发言[C].2003.

[45] 美国一心理咨询报告称战后驻伊美军士气低落[J/OL].[2005-07-21] http://news.xinhuanet.com/world/2005-07/21/content_3248076.htm.

[46] 驻伊美军回国后忙于心理咨询[J/OL].[2006-03-13]http://news.xinhuanet.com/mrdx/ 2006-03/13/content_4297579.htm.

[47] JULIAN BORGER E M, PATRICK WINTOUR.The hunt for weapons of mass destruction yields–nothing[N].The

Guardian,2003-09-25.

[48] GELLMAN B.Frustrated, U.S.Arms Team to leave Iraq[N].The Washington Post, 2003-05-11.

[49] 调查指美国伪造缴获伊拉克移动生化实验室情报[J/OL].2006, http://news.xinhuanet.com/newscenter/2006-04/13/content_4419548.htm.

[50] WARRICK J.Lacking biolabs, trailers carried case for war[N].The Washington Post, 2006-04-12.

[51] LINZER D.Search for banned arms in Iraq ended last month[N].The Washington Post, 2005.

[52] US chief Iraq arms expert quits[J/OL].[2004-01-24] http://news.bbc.co.uk/2/hi/americas/3424831.stm.

[53] DIAMOND J.Kay: ‘We were almost all wrong’[N].USA Today, 2004-01-29.

[54] Transcript:David Kay at Senate hearing[J/OL].[2004-01-28] http://edition.cnn.com/2004/US/01/28/kay.transcript/.

[55] Iraq survey group final report[M].2004.

[56] 汪明敏，谢海星，蒋旭光.美国情报监督机制研究[M].上海：光明日报出版社，2013.

[57] Executive Order 13328—Commission on the intelligence capabilities of the United States regarding weapons of mass destruction[M].2004.

[58] Unclassified version of the report of the commission on the intelligence capabilities of the United States regarding weapons of mass destruction[M].2005.

[59] 美调查委员会说有关伊拉克武器的情报“全错了”[J/OL].[2005-04-01] http://news.xinhuanet.com/world/2005-04/01/

content_2770734.htm.

[60] GOLDENBERG S.Iraq war my biggest regret, Bush admits[N].The Guardian, 2008.

[61] NICHOLS B.Tenet resigns as CIA director[N].USA Today, 2004-06-04.

[62] SCIOLINO E.As Bush ponders a Leader for the C.I.A., some say that no change is needed[N].The New Yorker Times, 2000-12-29.

[63] 乔治·沃克·布什.抉择时刻[M].北京：中信出版社，2011.

[64] GERHART A.Bush gives medal of freedom to ‘pivotal’ Iraq figures[N].The Washington Post, 2004- 02-15.

[65] GEORGE TENET B H.Slam dunk[M].At the center of the storm: The CIA during America’s time of crisis.Harper Perennial.2008.

[66] 迪克·切尼，莉兹·切尼.我的岁月：切尼回忆录[M].南京：译林出版社，2014.

[67] PELLEY S.George Tenet: At the center of the storm[J/OL].[2007-04-25] http://www.cbsnews.com/news/george-tenet-at-the-center-of-the-storm/.

[68] LYKE M L.Commander in chief ’s visit sets aircraft carrier’s crew abuzz[N].SEATTLE POST-INTELLIGENCER, 2003-05-01.

[69] MURPHY.‘Mission accomplished’ whodunit[J/OL].[2003-10-29] http://www.cbsnews.com/news/mission-accomplished-whodunit/.

[70] Commander in chief lands on USS Lincoln[J/OL].[2003-05-01] http://edition.cnn.com/2003/ALLPOLITICS/05/01/bush.carrier.landing/.

[71] MURPHY J.Text Of Bush speech[J/OL].[2013-01-05]http://www.cbsnews.com/news/text-of-bush-speech-01-05-2003/.

[72] 乔治·沃克·布什.抉择时刻[M].北京：中信出版社，2011.

[73] WILSON C.Searching for Saddam part I: The five families of Tikrit[M].Slate, 2010.

[74] WILSON C.Searching for Saddam Part III: the Brothers Musslit[M].Slate.2010.

[75] WILSON C.Searching for Saddam part IV: the fat man[M].Slate, 2010.

[76] GRIFFIN J.U.S.Intelligence Officer reveals secret story of Saddam Hussein's Capture[J/OL].[2008-12-12]http://www.foxnews.com/story/2008/12/12/us-intelligence-officer-reveals-secret-story-saddam-hussein-capture/.

[77] Saddam 'caught like a rat' in a hole[J/OL].[2003-12-15] http://edition.cnn.com/2003/WORLD/meast/12/14/sprj.irq.saddam.operation/.

[78] JULIAN BORGER G Y.Dead: the sons of Saddam[N].The Guardian, 2003-7-23.

[79] JULIAN BORGER J S.The last moments of Saddam's grandson[N].The Guardian, 2003-07-23.

[80] MARY LEONARD T R.For colonel, search mission was a perfect fit[N].The Boston Globe, 2003-12-16.

[81] WILSON C.Searching for Saddam Part II: Saddam family photos[M].Slate, 2010.

[82] REED B J.Formalizing the informal: a network analysis of an insurgency[D].University of Maryland, 2006.

[83] JEHL D.The capture of Hussein: intelligence; spy agencies vindicated after string of setbacks[N].The New York Times, 2013-12-15.

[84] President Bush's statement on execution of Saddam Hussein[M].2006.

[85] 萨达姆今日出庭受审六大罪状[J/OL].[2005-10-18]http://news.xinhuanet.com/world/2005-10/18/content_3639117.htm.

[86] 上任第一天奥巴马主攻中东和伊拉克问题[J/OL].[2009-01-20]http://world.people.com.cn/GB/57507/8702512.html.

[87] Iraq war in figures[J/OL].[2011-12-14]http://www.bbc.co.uk/news/world-middle-east-11107739.

[88] BLAIR D.Iraq war 10 years on: at least 116,000 civilians killed[N].The Telegraph, 2013-05-15.

[89] BAKER P.Grim Sequel to Iraq's War[N].The New York Times（中文版）, 2014-01-10.

[90] Excerpts from National Security Council report[N].The New York Times, 2006-03-13.

[91] Report of the Senate Select Committee on Intelligence on prewar intelligence assessments about postwar Iraq[M].2007.

[92] GERSTENZANG J.Bush was told twice of Iraq challenges[N].Los Angeles Times, 2007-05-26.

[93] WOODWARD B.Death of Osama bin Laden: phone call pointed U.S.to compound — and to 'the pacer'[N].The Washington Post, 2011-05-07.

[94] SOUZA P.President Barack Obama and Vice President Joe Biden, along with members of the national security team, receive an update on the mission against Osama bin Laden in the situation room[M].2011.

[95] 奥巴马就拉登被打死发表电视讲话[J/OL].[2011-05-02]http://www.chinadaily.com.cn/hqgj/2011-05/02/content_12430368.htm.

[96] Closing in on bin Laden[M].2011.

[97] ADAM GOLDMAN M A.The man who hunted Osama bin Laden[J/OL].[2011-07-05]http://news.yahoo.com/ap-enterprise-man-hunted-osama-bin-laden-040627805.html.

[98] Closing in on bin Laden: the one-acre complex[M].2011.

[99] THOMAS W.GILLESPIE J A A, ERIKA MARIANO, SCOTT MOSSLER, NOLAN JONES, MATT BRAUGHTON, JORGE GONZALEZ.Finding Osama bin Laden: an application of biogeographic theories and satellite imagery[J].MIT International Review, 2009.

[100] MATSON J.Can the science of biogeography find Osama bin Laden?[J].Scientific American, 2009.

[101] REARDON S.Geographers had predicted Osama's possible whereabouts[J/OL].[2011-05-02]http://news.sciencemag.org/education/2011/05/geographers-had-predicted-osamas-possible-whereabouts.

[102] JONES N.The 'Dynamite' Pentagon interview behind 'Zero Dark Thirty'[M].The Foreign Policy, 2013.

[103] GELL A.How a White House Flickr fail outed Bin Laden Hunter 'CIA John'[N].The New York Observer, 2011-07-12.

[104] CIA John Who hunted bin Laden photos[M].Cryptome, 2013.

[105] SOUZA P.President Barack Obama talks with members of the national security team at the conclusion of one in a series of meetings discussing the mission against Osama bin Laden[M].2011.

[106] DAVID HAGLUND A H, FORREST WICKMAN.Who are the people in Zero Dark Thirty?[M].Slate, 2013.

[107] 马克·欧文凯莫.艰难一日：海豹六队击毙本·拉登行动亲历[M].北京：中信出版社，2012.

[108] MILLER G.In ‘Zero Dark Thirty,’ she’s the hero; in real life, CIA agent’s career is more complicated[N].The Washington Post, 2012-12-11.

[109] 美军猎杀拉登中情局情报分析员功劳大被列首功[J/OL].[2011-07-07]http://www.chinanews.com/gj/2011/07-07/3165534.shtml.

[110] GELLMAN B.Enimies, foreign and domestic[M].Angler: The Cheney Vice Presidency.Penguin Books, 2008.

[111] MICHAEL KIRK J G, MIKE WISER.United States of secrets (Part One): The program[J/OL].[2014]http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/transcript-61/.

[112] MARC AMBINDER D B G.THE HORRORS BOOK[M].Deep state: inside the government secrecy industry.John Wiley & Sons, Inc., 2013.

[113] SNIDER L B.Unlucky Shamrock: recollections from the Church Committee’s investigation of NSA[J].Studies in Intelligence, 1999-2000, Winter 1999-2000.

[114] BAMFORD J.Muscle[M].Body of secrets: anatomy of the ultra-secret National Security Agency.Doubleday, 2001.

[115] 詹姆斯·班福德.秘密机构：美国国家安全局[M].北京：世界知识出版社，2003.

[116] COMMITTEE C, 1975-1976.

[117] 蒂姆·韦纳.中情局罪与罚：CIA60年秘史存灰[M].深圳：海天出版社，2009.

[118] 蒂姆·韦纳.中情局罪与罚：CIA60年秘史存灰[M].深圳：海天出版社，2009.

[119] The Watergate story: timeline[N].The Washington Post.

[120] Select Committee to study governmental operations, 1976.

[121] HUGHES K.A rough guide to Richard Nixon’s conspiracy theories[J/OL].http://millercenter.org/presidentialclassroom/exhibits/a-rough-guide-to-richard-nixons-conspiracy-theories#Tom_Charles_Huston.

[122] 尚之.尼克松比想象中更坏[J].南方人物周刊, 2012-07-02.

[123] CARL BERNSTEIN B W.Dean alleges Nixon knew of cover-up plan[N].The Washington Post, 1973-06-04.

[124] 蒂姆·韦纳.中情局罪与罚：CIA60年秘史存灰[M].深圳：海天出版社，2009.

[125] 汪明敏，谢海星，蒋旭光.美国情报监督机制研究[M].上海：光明日报出版社，2013.

[126] HERSH S M.Huge C.I.A.operation reported in U.S.against anti-war forces, other dissident[N].The New York Times,1974-12-21.

[127] 蒂姆·韦纳.中情局罪与罚：CIA60年秘史存灰[M].深圳：海天出版社，2009.

[128] “Family Jewels”[M]//CIA.

[129] CORN D.CIA releases the ‘family jewels’[N].The Washington Post, 2007-06-27.

[130] Chapter VII: The modern Senate, 1964-2002[M].200 notable days: senate stories, 1787 to 2002.U.S.government printing office, 2006.

[131] CHRIS PYLE[J/OL].http://americanradioworks.publicradio.org/features/noplacetohide/pyle.html.

[132] CAMPBELL K E.Rehearsal for Watergate[M].Senator Sam Ervin, last of the Founding Fathers.The University of North Carolina

Press, 2007.

[133] SCHEIPS P J.The role of federal military forces in domestic disorders, 1945-1992[M].2005.

[134] RISEN C.Spies among us[J].The American Scholar, 2009, Winter.

[135] BIGELOW M E.A short history of Army Intelligence[J/OL].[2012] https://www.fas.org/irp/agency/army/short.pdf.

[136] Cryptologic Almanac 50th Anniversary Series: Louis W.Tordella[J/OL].[2003] http://www.nsa.gov/public_info/_files/crypto_almanac_50th/Louis_W._Tordella.pdf.

[137] 詹姆斯·班福德.秘密机构：美国国家安全局[M].北京：世界知识出版社，2003.

[138] COMMITTEE C, 1975-1976.

[139] PINCUS W.This NSA history has a familiar ring to it[N].The Washington Post, 2014-05-19.

[140] 刘磊.冷战期间美国国会对隐蔽行动的监督研究[D].西安：陕西师范大学，2009.

[141] Overview of the Senate Select Committee on Intelligence responsibilities and activities.http://www.intelligence.senate.gov/about.html.

[142] Rules of procedure for the Select Committee on Intelligence United State Senate[M]//Senate U.S.government printing office, 2011.

[143] BAMFORD J.The agency that could be Big Brother[N].The New York Times, 2005-12-25.

[144] NSA inspector general report on email and internet data collection under Stellar Wind[M].2009.

[145] President discusses global war on terror following briefing

at CENTCOM[M].Office of the Press Secretary, 2006.

[146] BAMBORD J.Hunters[M].The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America Doubleday Publishing Group, 2008.

[147] CASTELLI E.New policy expected soon for sensitive information[M].Federal Times.2008.

[148] Designation and sharing of controlled unclassified information (CUI)[M].2008.

[149] Executive Order 13556 — controlled unclassified information[M].2010.

[150] Executive Order 13526 — classified national security information[M].2009.

[151] Executive Order 12958 — classified national security information[M].1995.

[152] WHITE L.Obama executive order issued to expedite declassification[M].Perspectives on History, 2010.

[153] Secrets, lies and America's spies[J].The Economist, 2013.

[154] KNIGHT J.Security clearance investigations[M].Encyclopedia of Espionage, Intelligence, and Security.

[155] COHEN S I.Sensitive compartmented information (SCI) appeals of access decisions under director of Central Intelligence directive no.6/4 (DCID 6/4).http://www.sheldoncohen.com/publications/sci_appeals_cia.htm.

[156] RICHELSON J T.The US Intelligence Community[M].Westview Press, 2011.

[157] Protection of Classified National Intelligence, including

sensitive compartmented information[M]//INTELLIGENCE OOTDON.Intelligence Community Directive 703.2013.

[158] GELLMAN B.How to angle[N].The Washington Post, 2008-10-19.

[159] Executive Order 12333 — United States intelligence activities[M].1981.

[160] MCCULLAGH D.Surveillance ‘partnership’ between NSA and telcos points to AT&T, Verizon[J/OL].[2013]http://www.cnet.com/news/surveillance-partnership-between-nsa-and-telcos-points-to-at-t-verizon/.

[161] Wiretap whistle-blower’s account[M].Wired, 2006.

[162] KRAVETS D.NSA leak vindicates AT&T whistleblower[M].Wired, 2013.

[163] MARC AMBINDER D B G.The flicker of a piercing eye[M].Deep state: inside the government secrecy industry.John Wiley & Sons, Inc., 2013.

[164] SANCHEZ J.What the Ashcroft “hospital showdown” on NSA spying was all about[J/OL].[2013-07]http://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about/.

[165] The hospital room showdown[M].SALON.Salon Media Group, 2007.

[166] DAN EGGEN P K.Gonzales hospital episode detailed[N].The Washington Post, 2007-05-16.

[167] GELLMAN B.Cheney shielded Bush from crisis[N].The Washington Post, 2008-09-15.

[168] 康多莉扎·赖斯.无上荣耀[M].长沙：湖南人民出版社，2014.

[169] The NSA program to detect and prevent terrorist attacks myth V.reality[M]//JUSTICE USDO, 2006.

[170] NAKASHIMA E.Legal memos released on Bush-era justification for warrantless wiretapping[N].The Washington Post, 2014-09-06.

[171] Unclassified report on the President's surveillance program[M].2009.

[172] ALLEN M.Bush's surveillance offensive[J].The Time, 2006.

[173] Lockheed Martin names James B.Comey General Counsel; succeeds Frank H.Menaker, who will retire[J/OL].[2005]http://www.prnewswire.com/news-releases/lockheed-martin-names-james-b-comey-general-counsel-succeeds-frank-h-menaker-who-will-retire-54688662.html.

[174] DRAKE BENNETT M R.Booz Allen, the world's most profitable spy organization[M].Bloomberg Business, 2013.

[175] NICK TABOREK D I.Booz Allen falls after employee Intel leak[M].Bloomberg Business, 2013.

[176] Booz Allen statement on reports of leaked information.[2013-06-09] http://www.boozallen.com/media-center/press-releases/2013/06/statement-reports-leaked-information-060913

[177] TOM HAMBURGER R O H J.Snowden case not the first embarrassment for Booz Allen, or D.C.contracting industry[N].The Washington Post, 2013-07-09.

[178] 丹·布赖奥迪.铁三角：透视凯雷集团的秘密世界[M].上海：上海远东出版社，2007.

[179] THORNTON E.Carlyle changes its stripes[M].Bloomberg Business, 2007.

[180] BRIODY D.Mr Clean[M].The iron triangle: inside the secret

world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[181] BRIODY D.The Politician, the Businessman, and the Unlucky Eskimos[M].The iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[182] IGNATIUS D.The president as businessman: the fancy financial footwork of George W.Bush[N].The New York Times, 2002-08-07.

[183] BRIODY D.Craterair[M].The iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[184] DRUM K.BUSH and the Board[M].Washington Monthly, 2003.

[185] BRIODY D.Cast of characters[M].The iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[186] BRIODY D.Family Business[M].The iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[187] GOODLEY S.Carlyle Group offers a slice of its own brand of controversy for $7bn[N].The Guardian, 2012-04-22.

[188] BRIODY D.Breaking the Bank[M].The Iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[189] OLIVER BURKEMAN J B.The ex-presidents’ club[N].The Guardian, 2001-10-30.

[190] Frank C.Carlucci.http://history.defense.gov/carlucci.shtml

[191] 丹·布赖奥迪.铁三角：透视凯雷集团的秘密世界[M].上海：上海远东出版社，2007.

[192] HEATH T.Carlyle Group is ready for its close-up[N].The Washington Post, 2011-06-04.

[193] BRIODY D.Big Guns[M].The iron triangle: inside the secret

world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[194] CLAIR J S.When war is swell: the Carlyle Group and the Middle East at War[J].CounterPunch, 2013.

[195] BRIODY D.9.11[M].The iron triangle: inside the secret world of the Carlyle Group.John Wiley & Sons, Inc., 2004.

[196] Spies for hire: Carlyle Group to become owner of “one of America’s largest private intelligence armies”.[2008] http://www.democracynow.org/2008/5/19/spies_for_hire_the_secret_world

[197] SHORROCK T.The CIA and the sacrifice of professionalism[M].Spies for hire: the secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[198] DALEY J.Carlyle quits Qinetiq with £240m profit[N].The independent, 2007-02-09.

[199] Books that shaped America.[2012] http://www.loc.gov/exhibits/books-that-shaped-america/index.html.

[200] ROGERS J.Author of ‘Fahrenheit 451,’ Ray Bradbury, dies at 91[J/OL].[2012-06-06] http://www.usnews.com/science/news/articles/2012/06/06/ray-bradbury-author-of-fahrenheit-451-dies.

[201] The Carlyle Group: C for capitalism[J].The Economist, 2003.

[202] ACKMAN D.The cost of being Osama bin Laden[J].Forbes, 2001,

[203] WRIGHT L.The Spymaster: can Mike McConnell fix America’s intelligence community?[J].New Yorker, 2008.

[204] SHORROCK T.Booz Allen Hamilton and “the shadow IC”[M].Spies for hire: the secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[205] SHANE S.MAN IN THE NEWS—John Michael McConnell; A member of the club[N].The New York Times, 2007-01-05.

[206] LEVY S.Battle of the clipper chip[N].The New York Times, 1994-06-12.

[207] SMITH C.Big Brother AL[J].WND Weekly, 2000.

[208] DRESSER M.NSA chief says code-breaker will enhance privacy[N].The Baltimore Sun,1994-05-04.

[209] MARKOFF J.At AT&T, no joy on clipper flaw[N].The New York Times, 1996-06-03.

[210] Clipper chip[M].Crypto museum.Paul Reuvers& Marc Simons, 2014.

[211] BLAZE M.Mykotronx MYK-78T (“Clipper”) escrowed encryption chip[M].2008.

[212] BLAZE M.AT&T TSD-3600E telephone security device (Clipper chip)[M].2008.

[213] ZETTER K.How a Crypto ‘backdoor’ pitted the tech world against the NSA[M].Wired.2013.

[214] MENN J.Secret contract tied NSA and security industry pioneer[J/OL].[2013-12-20]http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

[215] HUBLER D.McConnell to rejoin Booz Allen[N].Washington Technology, 2009-01-27.

[216] Dr.Shrader, EVP McConnell: “people to watch in 2010”[J/OL].[2010-01]http://www.boozallen.com/about/awards-recognition/2010/01/42852985.

[217] JOHN M.(MIKE) MCCONNELL.[2011] http://www.boozallen.com/about/leadership/executive-leadership/Mike-

McConnell.

[218] DAVID E.SANGER N P.After profits, defense contractor faces the pitfalls of cybersecurity[N].The New York Times （中文版）, 2013-06-19.

[219] GREENWALD G.Mike McConnell, the WashPost& the dangers of sleazy corporatism[M].SALON.Salon Media Group, 2010.

[220] President Bush nominates John Negroponte as Deputy Secretary of State and Vice Admiral Mike McConnell as Director of National Intelligence[J/OL].[2007] http://2001-2009.state.gov/r/pa/ei/wh/78411.htm.

[221] MCCULLAGH D.Senate endorses retroactive FISA immunity for warrantless wiretapping[J/OL].[2008]http://www.cnet.com/news/senate-endorses-retroactive-fisa-immunity-for-warrantless-wiretapping/#!

[222] MCCONNELL M.Mike McConnell on how to win the cyber-war we're losing[N].The Washington Post, 2010-02-28.

[223] BORGER J.Booz Allen Hamilton: Edward Snowden's US contracting firm[N].The Guardian, 2013-06-09.

[224] Booz Allen Hamilton, 2010.

[225] 秦伟江.解密斯诺登前雇主博思艾伦：美国“最高机密”外包商的57亿美元生意[N].21世纪经济报道, 2013-06-14.

[226] JOAN A.DEMPSEY, Executive Vice President.2013, http://www.boozallen.com/about/leadership/executive-leadership/dempsey.

[227] David Rubenstein And The Carlyle Group: The kings of capital[J].Forbes, 2012.

[228] DRAKE BENNETT C S, ROBERT LEVINSON Chart: How Booz Allen Hamilton swallowed Washington.[2013-06-13]http://www.businessweek.com/articles/2013-06-13/chart-how-booz-allen-

hamilton-swallowed-washington.

[229] Booz Allen’s contracting growth.[2013-07-08]http://www.washingtonpost.com/business/economy/booz-allens-contracting-growth/2013/07/08/ba5eb096-e823-11e2-a301-ea5a8116d211_graphic.html.

[230] Project Groundbreaker (NSA Contract).2009, http://www.crocodyl.org/spies_for_hire/project_groundbreaker_nsa_contract.

[231] TRW completes $975-Million BDM buy[N].Los Angeles Times, 1997-12-27.

[232] DANA PRIEST W M A.Top secret America: Part 2: National Security Inc.[N].The Washington Post, 2010-07-20.

[233] ARMSTRONG G.Mapping the shadow government: Booz Allen Hamilton[M].LittleSis, 2013.

[234] Lobbying Expenses for Booz Allen Hamilton.http://www.opensecrets.org/lobby/clientsum.php?id=D000032046&year=2002.

[235] JAMES ALLEN, Senior vice president.2012, https://www.boozallen.com/about/leadership/executive-leadership/James-Allen.

[236] RICHARD J.WILHELM, Executive vice president.2013, https://www.boozallen.com/about/leadership/executive-leadership/Richard-Wilhelm.

[237] TERRY THOMPSON, Vice president.2014, https://www.boozallen.com/about/leadership/executive-leadership/Terry-Thompson.

[238] KELLY S.Intelligence goes private: the case file on Joan Dempsey[M].Security Clearance.CNN, 2012.

[239] 田实.美国中央情报局局长[M].北京：军事科学出版社，

2008.

[240] ANTONY BARNETT S H.Bush ally set to profit from the war on terror[M].The Observer.Guardian News and Media Limited.2003.

[241] Board of Advisors.http://www.insaonline.org/i/a/l/Board_of_Advisors.aspx.

[242] Board of Directors.http://www.insaonline.org/i/a/L/BOD/i/a/l/Board_of_Directors.aspx.

[243] Executive Committee.http://www.insaonline.org/i/a/L/ec/i/a/l/Executive_Committee.aspx.

[244] INSA Corporate Members.http://www.insaonline.org/i/M/CM/i/b/a/Corporate_Members.aspx?hkey=d158a9f6-6a42-4411-a126-cb1799e6f10a.

[245] HENRY A."Trey" Obering III, Senior vice president.2012, https://www.boozallen.com/about/leadership/executive-leadership/Trey-Obering.

[246] STEVE SOULES, Senior vice president.2012, http://www.boozallen.com/about/leadership/executive-leadership/Steve-Soules.

[247] Transitioning Military.http://www.boozallen.com/careers/find-your-job/military.

[248] Top 100 Military Friendly Employers.http://www.gijobs.com/top100pr.aspx.

[249] SHORROCK T.Afterword[M].Spies for hire: the secret world of intelligence outsourcing.SIMON & SCHUSTER PAPERBACKS, 2008.

[250] CHATTERJEE P.How Booz Allen Made the Revolving Door Redundant[J/OL].2013, http://www.ipsnews.net/2013/06/how-booz-allen-made-the-revolving-door-redundant/.

[251] LOEB V.Test of Strength[M].The Washington Post Magazine, 2001.

[252] GORMAN S.System Error[N].The Baltimore Sun, 2006-01-29.

[253] H.R.1588 (108th): National Defense Authorization Act for fiscal year 2004[M].2003.

[254] NSA whistleblower Thomas Drake prevails against charges in unprecedented Obama Admin crackdown[J/OL].[2012] http://www.democracynow.org/2012/3/21/in_unprecedented_obama_admin_crackdown_nsa.

[255] SHORROCK T.The NSA, 9/11, and the business of data mining[M].Spies for hire: the secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[256] ONLEY D S.At NSA, mum's the word on Groundbreaker's details[M].GCN.2001.

[257] SHORROCK T.Carlyle Group may buy major CIA contractor: Booz Allen Hamilton[J].ZNet, 2008.

[258] SHORROCK T.The rise of the national surveillance state[M].Spies for hire: The secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[259] GORMAN S.Computer ills hinder NSA[N].The Baltimore Sun, 2006-02-26.

[260] MAYER J.THE SECRET SHARER: Is Thomas Drake an enemy of the state?[J].The New Yorker, 2011.

[261] GORMAN S.NSA rejected system that sifted phone data legally[N].The Baltimore Sun, 2006-05-18.

[262] CATERINICCHIA D.NSA taps SAIC for trailblazer[M].FCW, 2002.

[263] GORMAN S.Little-known contractor has close ties with staff of NSA[N].The Baltimore Sun, 2006-01-29.

[264] National security agency whistle-blower william Binney on growing state surveillance[J/OL].2012, http://www.democracynow.org/2012/4/20/whistleblower_the_nsa_is_lying_us.

[265] GORMAN S.Costly NSA initiative has a shaky takeoff[N].The Baltimore Sun, 2007-02-11.

[266] DARCY D.CSC forms cyber advisory committee[J].Washington Business Journal, 2009.

[267] “旋转门”在各国屡遭诟病美日等国立法监管[J/OL].[2013-08-12] http://finance.chinanews.com/cj/2013/08-12/5150526.shtml.

[268] Jacques Gansler.http://www.cpppe.umd.edu/About/jgbio.html

[269] GOLDFARB Z A.Should this marriage be saved?[N].The Washington Post, 2008-02-04.

[270] How Booz & Company develops and markets consulting concepts[J/OL].[2013] http://bloomgroup.com/content/how-booz-co-develops-and-markets-consulting-concepts.

[271] SHORROCK T.Conclusion: ideology, oversight, and the costs of secrecy[M].spies for hire: the secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[272] SHORROCK T.A short history of intelligence outsourcing[M].Spies for hire: the secret world of intelligence outsourcing.Simon & Schuster Paperbacks, 2008.

[273] GOULD J.Reserve lt.allegedly lied to get base housing[N].Army Times, 2011-01-23.

[274] MOORE J.Air Force suspends Booz Allen's San Antonio office[J/OL].2012, http://www.federalnewsradio.com/130/2738345/Air-Force-suspends-Booz-Allens-San-Antonio-office.

[275] CHACKO S.Air Force lifts suspension of Booz Allen's San Antonio office[J/OL].2012, http://www.federaltimes.com/article/20120416/ACQUISITION03/204160305/Air-Force-lifts-suspension-Booz-Allen-s-San-Antonio-office.

[276] GREENWALD G.Ten days in Hong Kong[M].No place to hide: Edward Snowden, the NSA, and the US surveillance state.Metropolitan Books, 2014.

[277] KRISTINA COOKE J S.Snowden as a teen online: anime and cheeky humor[J/OL].2013, http://www.reuters.com/article/2013/06/12/us-usa-security-snowden-anime-idUSBRE95B14B20130612.

[278] GREENBERG A.An NSA coworker remembers the real Edward Snowden: 'a genius among geniuses'[J].Forbes, 2013.

[279] SUZANNA ANDREWS B B, SARAH ELLISON.The Snowden saga: a shadowland of secrets and light[M].Vanity Fair.Condé Nast Digital, 2014.

[280] CAROL D.LEONNIG J J, MARC FISHER.Tracking Edward Snowden, from a Maryland classroom to a Hong Kong hotel[N].The Washington Post, 2013-06-16.

[281] NSA contractor: 'I know I have done nothing wrong'[N].USA TODAY, 2013-06-09.

[282] MATTHEW MOSK J G M, SHUSHANNAH WALSHE, LEE FERRAN.Timeline: Edward Snowden's life as we know it[J/OL].2013, http://abcnews.go.com/Blotter/timeline-edward-snowdens-life/story?id=19394487.

[283] National centers of academic excellence.[2013] http://

www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

[284] KROLL A.Community college says NSA whistleblower Edward Snowden took no “cyber-related classes”[M].Mother Jones, 2013.

[285] YOSHIDA R.Snowden web manga profile still online[J/OL].2013, http://www.japantimes.co.jp/news/2013/06/15/national/02-profile-paints-snowden-as-manga-anime-gun-girlish-geek-with-list-of-likes/#.UycWx_mSxSx.

[286] GELLMAN B.Edward Snowden, after months of NSA revelations, says his mission’s accomplished[N].The Washington Post, 2013-12-24.

[287] JOHN M.BRODER S S.For Snowden, a life of ambition, despite the drifting[N].The New York Times, 2013-06-13.

[288] THETRUEHOOHA.Tell me about...A career in the military (or overseas)![M].2006.

[289] HOSENBALL M.NSA contractor hired Snowden despite concerns about resume discrepancies[J/OL].2013, REUTERS(http://www.reuters.com/article/2013/06/21/us-usa-security-snowden-idUSBRE95K01J20130621.

[290] JEAN MARBELLA S B, DAVID S.CLOUD.Details about Edward Snowden’s life in Maryland emerge[N].The Baltimore Sun, 2013-06-10.

[291] FRANKLIN J.Edward Snowden evolved from gaming geek to conscientious whistleblower[J/OL].2014,http://www.truth-out.org/news/item/20983-edward-snowden-evolved-from-gaming-geek-to-conscientious-whistleblower-how-a-high-tech-spy-came-in-from-the-cold.

[292] THETRUEHOOHA.Okay, okay.This is getting real.I had...a vision[M].2008.

[293] GLENN GREENWALD E M, LAURA POITRAS.Edward Snowden: the whistleblower behind the NSA surveillance revelations[N].The Guardian, 2013-06-09.

[294] 李杨.多少保安哥变身“励志哥”[N].新快报，2012-09-18.

[295] BLASEY L.Man behind NSA leak previously worked at univ.facility[N].The Diamondback, 2013-06-09.

[296] PETER FINN G M, ELLEN NAKASHIMA.Investigators looking into how Snowden gained access at NSA[N].The Washington Post, 2013-06-11.

[297] Clues to future Snowden leaks found in his past[M].WashingtonsBlog.2014.

[298] DARCY O.Snowden earned annual salary of $29k in first NSA job[J/OL].2013, http://www.campusreform.org/?ID=4843.

[299] THETRUEHOOHA.state school vs.expensive college[M].2006.

[300] About CASL.http://www.casl.umd.edu/about.

[301] HUSLIN A.Intelligence agency joins U-Md.Research center[N].The Washington Post, 2008-06-16.

[302] ROPPOLO M.Snowden case shows ‘top secret’ clearance checks not foolproof[J/OL].2013.

[303] KATZ A.Potential blind spots in clearance process that gave Snowden top-secret access[M].Time, 2013.

[304] THETRUEHOOHA.Overseas employment?[M].2006.

[305] HARDING L.How Edward Snowden went from loyal NSA contractor to whistleblower[N].The Guardian, 2014-01-31.

[306] ADAM GELLER B W.Edward Snowden’s background surrounded by spycraft[J/OL].2013, http://

www.huffingtonpost.com/2013/06/15/edward-snowden-background_n_3446904.html.

[307] There is an NSA/CIA hybrid agency that may explain Snowden’s involvement in sigint and humint[M].Leask Source.2013.

[308] FORD T H.A History of America’s National Reconnaissance Office, Part 1[M].codshitcom, 2005.

[309] BAMFORD J.Heart[M].Body of secrets: anatomy of the ultra-secret National Security Agency.DOUBLEDAY.2001.

[310] W.BROWN D.Inside the secret world of America’s top eavesdropping spies[M].The Week, 2012.

[311] KAIHLA P.Weapons of the Secret War[J].Business 20, 2001, 11.

[312] LICHTBLAU E.Spy suspect may have revealed U.S.bugging[N].Los Angeles Times, 2001-04-17.

[313] 卢克·哈丁.斯诺登档案[M].北京：金城出版社，2014.

[314] ACOB APPELBAUM N B, HUBERT GUDE, RALF NEUKIRCH, RENÉ PFISTER, LAURA POITRAS, MARCEL ROSENBACH, JÖRG SCHINDLER, GREGOR PETER SCHMITZ, HOLGER STARK.Embassy espionage: The NSA’s secret spy hub in Berlin[M].Der Spiegel, 2013.

[315] Obama awards freedom medals to Bush, Merkel, Buffett[J/OL].2011, http://www.reuters.com/article/2011/02/15/us-obama-medals-idUSTRE71E60P20110215.

[316] APPLEBAUM A.Why did the NSA tap Angela Merkel’s cellphone?[M].Slate, 2013.

[317] Media reports suggest Obama knew NSA spied on Merkel[J/OL].2013, http://www.dw.de/media-reports-suggest-obama-knew-nsa-spied-on-merkel/a-17185662.

[318] Barack Obama knew about NSA’s spying on Angela Merkel: Report[M].The Economic Times, 2013.

[319] PAUL LEWIS P O.NSA denies discussing Merkel phone surveillance with Obama[N].The Guardian, 2013-10-27.

[320] MARC HUJER H S.Former NSA Director: ‘shame on us’[M].Der Spiegel, 2014.

[321] BAKER S.Allies aren’t alway friends[N].The New York Times, 2013-12-19.

[322] PITZKE M.US on spying scandal: ‘allies aren’t always friends’[M].Der Spiegel, 2013.

[323] ERLANGER S.Outrage in Europe grows over spying disclosures[N].The New York Times（中文版）, 2013-07-02.

[324] DUNCAN CAMPBELL CM, KIM SENGUPTA, NIGEL MORRIS, TONY PATTERSON.Revealed: Britain’s ‘secret listening post in the heart of Berlin’[N].The Independent, 2013-11-05.

[325] Photo gallery: Spies in the embassy[M].2013.

[326] SCOTT SHANE C D.Résumé shows Snowden honed hacking skills[N].The New York Times（中文版）, 2013-07-05.

[327] RISEN J.Snowden says he took no secret files to russia[N].The New York Times, 2013-10-17.

[328] SCHMITT E.C.I.A.Disputes early suspicions on Snowden[N].The New York Times, 2013-10-11.

[329] ANDERSON M.Who is Ed Snowden? Friend shares memories, offers support for NSA leaker[J/OL].2013, http://www.timesfreepress.com/news/2013/jun/12/who-is-ed-snowden/.

[330] HOSENBALL M.Snowden downloaded NSA secrets while working for Dell, sources say[J/OL].2013,http://www.reuters.com/

article/2013/08/15/usa-security-snowden-dell-idUSL2N0GF11220130815.

[331] 卢克·哈丁.斯诺登档案[M].金城出版社，2014.

[332] JOHNSON C.Chatting about Japan with Snowden, the NSA whistle-blower[N].The Japan Times, 2013-06-18.

[333] DANIEL BATES M Z, HELEN POW.The beautiful ballerina girlfriend whistleblower Ed Snowden was set to wed before he left her in Hawaii and fled to Hong Kong to leak NSA secrets.Now she says she feels ‘adrift’[N].Daily Mail, 2013-06-10.

[334] Personnel reduction expected at Misawa.2014, http://www.misawa.af.mil/news/story.asp?id＝123401836.

[335] Misawa Security Operations Center.2009, http://www.misawa.af.mil/library/factsheets/factsheet.asp?id＝14098.

[336] DAVID ALEXANDER A S.Budget cuts to slash U.S.Army to smallest since before World War Two[J/OL].2014, http://www.reuters.com/article/2014/02/24/us-usa-defense-budget-idUSBREA1N1IO20140224.

[337] CICCARONE P.708th Military Intelligence Detachment says farewell[J/OL].2014, http://www.misawa.af.mil/news/story.asp?id＝123413210.

[338] GITTLER J.Security Hill marks 50 years of silent service[N].Stars and Stripes, 2003-09-07.

[339] LIMON A R.Misawa to tear down massive ‘Elephant Cage’ antennae[N].Stars and Stripes, 2012-11-19.

[340] WILKINSON J.Japan and Project Echelon: Report on secretive U.S.Military Base in Misawa, Aomori Prefecture[J].The New Observer, 2000.

[341] NELSON D.Edward Snowden ‘attended hacking course in

India'[N].The Guardian, 2013-12-04.

[342] MACASKILL E.Edward Snowden, NSA files source: 'If they want to get you, in time they will'[N].The Guardian, 2013-06-09.

[343] Central Security Service Insignia.2012, http://www.nsa.gov/about/central_security_service/css_insignia.shtml.

[344] BAMFORD J.The secret war[M].Wired, 2013.

[345] PIKE J.Regional SIGINT Operations Center Kunia.2000, http://fas.org/irp/facility/kunia.htm.

[346] NSA/CSS Unveils New Hawaii Center: Designed to Boost Intelligence Integration, Collaboration.2012, http://www.nsa.gov/public_info/press_room/2012/a4_hawaii_final.shtml.

[347] History of NIOC Hawaii.http://www.public.navy.mil/fcc-c10f/niochi/Pages/AboutUs.aspx.

[348] DAVID E.SANGER E S.Snowden used low-cost tool to best N.S.A.[N].The New York Times, 2014-02-08.

[349] VOGEL S.For Intelligence Officers, A wiki way to connect dots[N].The Washington Post, 2009-08-27.

[350] Intellipedia usage statistics.[2014] https://www.muckrock.com/foi/united-states-of-america-10/intellipedia-usage-statistics-10058/#1017757-responsive-documents.

[351] HOSENBALL M.NSA chief says Snowden leaked up to 200,000 secret documents[J/OL].2013, http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114.

[352] TABASSUM ZAKARIA W S.After 'cataclysmic' Snowden affair, NSA faces winds of change[J/OL].2013,http://www.reuters.com/article/2013/12/13/us-usa-security-nsa-idUSBRE9BC0YZ20131213.

[353] GREENWALD G.Contact[M].No place to hide: Edward Snowden, the NSA, and the US Surveillance State.Metropolitan Books, 2014.

[354] MAASS P.How Laura Poitras helped Snowden spill his secrets[N].The New York Times, 2013-08-13.

[355] GREENWALD G.U.S.filmmaker repeatedly detained at border[M].SALON.Salon Media Group, 2012.

[356] US No-Fly list doubles in one year[J/OL].2012, http://www.foxnews.com/us/2012/02/02/ap-exclusive-us-no-fly-list-doubles-in-1-year/.

[357] Father of terror suspect reportedly warned U.S.about son[J/OL].2009, http://www.foxnews.com/story/2009/12/26/father-terror-suspect-reportedly-warned-us-about-so-1157956136/.

[358] 格伦·格林沃尔德.无处可藏：斯诺登、美国国安局与全球监控[M].北京：中信出版社，2014.

[359] POULSEN K.Snowden’s first move against the NSA was a party in Hawaii[M].Wired, 2014.

[360] LAM L.Snowden sought Booz Allen job to gather evidence on NSA surveillance[N].South China Morning Post, 2013-06-24.

[361] 卢克·哈丁.斯诺登档案[M].金城出版社，2014.

[362] GELLMAN B.Code name ‘Verax’: Snowden, in exchanges with Post reporter, made clear he knew risks[N].The Washington Post, 2013-06-09.

[363] GREENWALD G.“I have been to the darkest corners of government, and what they fear is light”[M].SALON.Salon Media Group, 2014.

[364] Best Law Schools.2014, http://grad-schools.usnews.rankingsandreviews.com/best-graduate-schools/top-

law-schools/law-rankings?int＝992008.

[365] REITMAN J.Snowden and Greenwald: The men who leaked the secrets[M].Rolling Stone.2013.

[366] ENGEL P.Guardian bypasses old observer space, picking onion as neighbor[N].The Observer, 2011-06-29.

[367] 卢克·哈丁.斯诺登档案[M].金城出版社，2014.

[368] WOOLF N.How The Guardian broke the Snowden story[M].The Atlantic, 2013.

[369] WITT E.The Guardian in America is going to be British this time[N].The Observer, 2011-06-27.

[370] 卢克·哈丁.斯诺登档案[M].金城出版社，2014.

[371] MACASKILL E.Edward Snowden: how the spy story of the age leaked out[N].The Guardian, 2013-06-12.

[372] DAN ROBERTS S A.Anger swells after NSA phone records court order revelations[N].The Guardian, 2013-06-07.

[373] HARDING L.Writing the Snowden files: ‘The paragraph began to self-delete’[N].The Guardian, 2014-02-20.

[374] GREENWALD G.NSA collecting phone records of millions of Verizon customers daily[N].The Guardian, 2013-06-05.

[375] BLAKE A.Administration: NSA phone record collection vital to fighting terrorism[N].The Washington Post, 2013-06-06.

[376] HARRIS S.3 Degrees of separation is enough to have you watched by the NSA[M].The Foreign Policy, 2013.

[377] SIOBHAN GORMAN E P, JANET HOOK.U.S.collects vast data trove[N].The Wall Street Journal, 2013-06-07.

[378] WHITTAKER Z.NSA ‘top secret’ spying order affects

millions of Americans: FAQ[J/OL].[2013] http://www.zdnet.com/nsa-top-secret-spying-order-affects-millions-of-americans-faq-7000016489/.

[379] CHARLIE SAVAGE E W.N.S.A.Said to gather users' online data[N].The New York Times, 2013-06-07.

[380] SAVAGE C.Senators say Patriot Act is being misinterpreted[N].The New York Times, 2011-05-26.

[381] WHITTAKER Z.Senator: "The 'real' Patriot Act is classified"[J/OL].2011, http://www.zdnet.com/blog/igeneration/senator-the-real-patriot-act-is-classified/10286.

[382] Statement of U.S.Senator Russ Feingold On reauthorization of the USA Patriot Act[M].Senate Judiciary Committee, 2009.

[383] FRIEDERSDORF C.Russ Feingold tried to warn us about section 215 of the Patriot Act[M].The Atlantic, 2013.

[384] TERKEL A.Watch the one senator who voted against The Patriot Act warn what would happen[N].The Huffington Post, 2013-06-07.

[385] HAGAN J.The United States of America vs.Bill Keller[M].New York Magzine.2006.

[386] Polls: Kerry won debate[J/OL].2004, http://www.cnn.com/2004/ALLPOLITICS/10/03/election.poll/.

[387] CALAME B.Eavesdropping and the election: An answer on the question of timing[N].The New York Times, 2006-08-13.

[388] SULLIVAN M.Lessons in a surveillance drama redux[N].The New York Times, 2013-11-09.

[389] KEYS M.Government pressured New York Times to withhold NSA surveillance story[M].TheBlot, 2014.

[390] ISIKOFF M.The whistle-blower who exposed warrantless wiretaps[M].Newsweek, 2008.

[391] Thomas Tamm[J/OL].[2013] http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-tamm/.

[392] Bush's Law: Eric Lichtblau on exposing the NSA's warrantless wiretapping program and how the White House pressured the New York Times to kill the story[J/OL].2008, http://www.democracynow.org/2008/4/1/exclusivebushs_law_eric_lichtblau_on_exposing.

[393] FOLKENFLIK D.'New York Times' Editor: Losing Snowden scoop 'really painful'[J/OL].2014, http://www.npr.org/2014/06/05/319233332/new-york-times-editor-losing-snowden-scoop-really-painful.

[394] JAMES RISEN E L.Bush Lets U.S.Spy on callers without courts[N].The New York Times, 2005-12-16.

[395] President Bush's weekly radio address[N].The Washington Post, 2005-12-17.

[396] Bush says he signed NSA wiretap order Adds he OK'd program more than 30 times, will continue to do so[J/OL].2005, http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/.

[397] President discusses global war on terror at Kansas State University[M].2006.

[398] FOLKENFLIK D.'Times' held story on U.S.surveillance for a year[J/OL].2005, http://www.npr.org/templates/story/story.php?storyId=5058710.

[399] SHERMAN G.Risen gave Times a non-disclosure on wiretap book[M].The Observer.2006.

[400] How we broke the NSA story[M].Salon, 2013.

[401] NAKASHIMA E.Former NSA executive Thomas A.Drake may pay high price for media leak[N].The Washington Post, 2010-07-14.

[402] Edward Loomis[J/OL].2013, http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-edward-loomis/.

[403] REILLY J.Feds vow to hunt down NSA leaker as they fear he is attempting to defect to China with America's most sensitive secrets[N].Daily Mail, 2013-06-13.

[404] HOFSCHNEIDER A.Hawaii real estate agent: Snowden left on May 1[J/OL].2013, http://bigstory.ap.org/article/hawaii-real-estate-agent-snowden-left-may-1.

[405] KURTZ H.Washington Post shutters last U.S.bureaus[N].The Washington Post, 2009-11-24.

[406] CALDERONE M.WaPo's Gellman joins Time[M].Politico, 2010.

[407] AULETTA K.Freedom of Information[M].New Yorker, 2013.

[408] Barton Gellman[J/OL].2014, http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-barton-gellman/.

[409] Reporter had to decide if Snowden leaks were 'the real thing'[J/OL].[2013] http://www.npr.org/2013/09/11/221359323/reporter-had-to-decide-if-snowden-leaks-were-the-real-thing.

[410] Staff Home Page: Barton Gellman.2005, http://www.washingtonpost.com/wp-dyn/admin/staff/gellmanbart/.

[411] WANG A.Spilling secrets: Barton Gellman'82[N].The Daily Princetonian, 2013-10-14.

[412] GELLMAN B.Odyssey of frustration[N].The Washington

Post, 2003-05-18.

[413] GELLMAN B.Covert unit hunted for Iraqi arms[N].The Washington Post, 2003-06-13.

[414] CALDERONE M.Washington Post began PRISM story three weeks ago, heard Guardian's 'footsteps'[J/OL].[2013] http://www.huffingtonpost.com/2013/06/07/washington-post-prism-guardian_n_3402883.html.

[415] JACOBSON L.Reporting on government surveillance[M].Princeton Alumni Weekly, 2014.

[416] PETERSON A.Post reporter: Here's why we refused the NSA's demand to censor the names of PRISM companies[N].The Washington Post, 2013-10-09.

[417] BARTON GELLMAN L P.U.S., British intelligence mining data from nine U.S.Internet companies in broad secret program[N].The Washington Post, 2013-06-07.

[418] BOTT E.The real story in the NSA scandal is the collapse of journalism[J/OL].2013, http://www.zdnet.com/the-real-story-in-the-nsa-scandal-is-the-collapse-of-journalism-7000016570/.

[419] GLENN GREENWALD E M.NSA Prism program taps in to user data of Apple, Google and others[N].The Guardian, 2013-06-07.

[420] STEPHEN BRAUN A F, JACK GILLUM, MATT APUZZO.Secret to prism program: even bigger data seizure[J/OL].2013, http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure.

[421] ERIC LICHTBLAU J R, MARK MAZZETTI.Reported drop in surveillance spurred a law[N].The New York Times, 2007-08-11.

[422] LEE T B.How Congress unknowingly legalized PRISM in 2007[N].The Washington Post, 2013-06-06.

[423] LIZZA R.State of Deception[M].The New Yorker, 2014.

[424] NSA fears prompt germany to end verizon contract[J/OL].2014, http://bigstory.ap.org/article/nsa-fears-prompt-germany-end-verizon-contract.

[425] NEWMAN L H.The German government doesn't trust verizon to protect its data from the NSA[M].Slate, 2014.

[426] LEYDEN J.CIA-funded upstart: The truth about Prism and NSA's web snooping[M].The Register, 2013.

[427] MCCULLAGH D.No evidence of NSA's 'direct access' to tech companies[J/OL].[2013] http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/.

[428] ROBERT O'HARROW JR.E N, BARTON GELLMAN U.S., company officials: Internet surveillance does not indiscriminately mine data[N].The Washington Post, 2013-06-08.

[429] RUSHE D.Facebook and Google insist they did not know of Prism surveillance program[N].The Guardian, 2013-06-08.

[430] MACASKILL E.NSA paid millions to cover Prism compliance costs for tech companies[N].The Guardian, 2013-08-23.

[431] BALL J.NSA's Prism surveillance program: how it works and what it can do[N].The Guardian, 2013-06-08.

[432] MILLER C C.Tech companies, bristling, concede to government surveillance efforts[N].The New York Times（中文版）, 2013-06-09.

[433] GLENN GREENWALD E M, LAURA POITRAS, SPENCER ACKERMAN, DOMINIC RUSHE.Microsoft handed the NSA access to encrypted messages[N].The Guardian, 2013-07-12.

[434] MILLER C C.Secret court ruling put tech companies in data bind[N].The New York Times（中文版）, 2013-06-15.

[435] STROHM C.Yahoo faced $250,000-Day Fine for not giving U.S.data[M].Bloomberg Business, 2014.

[436] RISEN J.Report indicates more extensive cooperation by Microsoft on surveillance[N].The New York Times（中文版）, 2013-07-12.

[437] NICK WINGFIELD J R.Quest for pools of data binds silicon Valley and spy agency[N].The New York Times（中文版）, 2013-06-21.

[438] MASNICK M.More details on PRISM revealed; Twitter deserves Kudos For refusing to give in[J/OL].2013, https://www.techdirt.com/articles/20130608/09315223373/more-details-prism-revealed-twitter-deserves-kudos-refusing-to-give.shtml.

[439] MARTIN S.Twitter notably absent from NSA PRISM list[N].USA Today, 2013-06-07.

[440] KIRK J.Snowden's email provider, Lavabit, shutters citing legal pressure[M].PCWorld, 2013.

[441] LEVISON L.2014, http://lavabit.com/

[442] RIBEIRO J.After Lavabit, Silent Circle also shuts down its encrypted email service[M].PCWorld, 2013.

[443] TIMBERG C.NSA slide shows surveillance of undersea cables[N].The Washington Post, 2013-07-10.

[444] SIOBHAN GORMAN J V-D.New details show broader NSA surveillance reach[N].The Wall Street Journal, 2013-08-20.

[445] HEIL E.What's the deal with NSA's operation names?[N].The Washington Post, 2013-10-22.

[446] CRAIG TIMBERG B G.NSA paying U.S.companies for access to communications networks[N].The Washington Post, 2013-08-29.

[447] 詹姆斯·班福德.秘密机构：美国国家安全局[M].北京：世界知识出版社，2003.

[448] ANTON GEIST S G, HENRIK MOLTKE, LAURA POITRAS.NSA ‘third party’ partners tap the Internet backbone in global surveillance program[M].Information, 2014.

[449] LAURA POITRAS M R, HOLGER STARK.Ally and target: US intelligence watches Germany closely[M].DER SPIEGEL.2013.

[450] BARTON GELLMAN J T, ASHKAN SOLTANI.In NSA-intercepted data, those not targeted far outnumber the foreigners who are[N].The Washington Post, 2014-07-05.

[451] Statistical transparency report regarding use of National Security Authorities - annual statistics for calendar year 2013[M]// Intelligence Ootdon, 2014.

[452] HIGGINS P.Intelligence agency attorney on how “multi-communication transactions” allowed for domestic surveillance[J/OL].2013, https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed.

[453] Report on the surveillance program operated pursuant to section 702 of the foreign intelligence surveillance act[M]//Board Paclo, 2014.

[454] DAVID E.SANGER E S.N.S.A.Imposes rules to protect secret data stored on its networks[N].The New York Times （中文版）, 2013-07-22.

[455] SCOTT SHANE J W.Earlier denials put intelligence chief in awkward position[N].The New York Times, 2013-06-11.

[456] LEDERMAN J.Intelligence chief blasts NSA document leaks[J/OL].2013, http://bigstory.ap.org/article/intelligence-chief-blasts-nsa-document-leaks.

[457]　迪克·切尼，莉兹·切尼.我的岁月：切尼回忆录[M].南京：译林出版社，2014.

[458] WINDREM R.What is a PDB: A brief explanation of the top secret document[J/OL].2004, http://www.nbcnews.com/id/4724611/ns/us_news-security/t/what-pdb/#.VCFxcvmSxSx.

[459] PINCUS W.Measuring a president's approach on foreign policy[N].The Washington Post, 2012-01-16.

[460] The Evolution of the President's Daily Brief.2014, https://www.cia.gov/news-information/featured-story-archive/2014-featured-story-archive/the-evolution-of-the-presidents-daily-brief.html.

[461] SOUZA P.President Barack Obama receives the Presidential daily briefing from Robert Cardillo, Deputy Director of national intelligence for intelligence integration, in the Oval Office, Jan.31, 2012.Part of the briefing was done using a tablet computer[M].2012.

[462] MILLER G.Oval Office iPad: President's daily intelligence brief goes high-tech[N].The Washington Post, 2012-04-12.

[463] MAZMANIAN A.A wish list for a digitized President's daily brief[M].FCW, 2014.

[464] C.LAWRENCE MEADOR V G C.Rethinking the President's daily intelligence brief[J].Studies in Intelligence, 2013, 57(4).

[465] THIESSEN M A.Why is Obama skipping more than half of his daily intelligence meetings?[N].The Washington Post, 2012-09-10.

[466] GREENWALD G.Collect It All[M].No Place to hide: Edward Snowden, the NSA, and the US surveillance state.Metropolitan Books, 2014.

[467] Transcript provided by Federal News Service.2013, http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

[468] PETER BAKER D E S.Obama calls surveillance programs legal and limited[N].The New York Times（中文版）, 2013-06-08.

[469] IGNATIUS D.Snowden exposed policies approved by Congress, courts[N].The Washington Post, 2013-06-12.

[470] FRIEDMAN T L.Blowing a whistle[N].The New York Times, 2013-06-11.

[471] President Obama defends NSA spying.2013, http://www.buzzfeed.com/buzzfeedpolitics/president-obama-defends-nsa-spying.

[472] GREENWALD G.Fisa court oversight: a look inside a secret and empty process[N].The Guardian, 2013-06-19.

[473] BALKIN J M.The inspector General’s report and The Horse that is already out of the barn door[M].Balkinization.2013.

[474] AMBINDER M.The NSA Organization Chart[M].

[475] NSA slides explain the PRISM data-collection program[N].The Washington Post, 2013-06-06.

[476] BARTON GELLMAN T L.Inner workings of a top-secret spy program[N].The Washington Post, 2013-06-29.

[477] BAMFORD J.The NSA is building the country’s biggest spy center (Watch What You Say)[M].Wired, 2012.

[478] BAMFORD J.Connecting the dots on PRISM, phone surveillance, and the NSA’s massive spy Center[M].Wired, 2013.

[479] FASCIA: The NSA’s huge trove of location records[N].The Washington Post, 2013-12-04.

[480] GLENN GREENWALD J B.The top secret rules that allow NSA to use US data without a warrant[N].The Guardian, 2013-06-20.

[481] DAVID E.SANGER S S.Job title key to inner access Held by

leaker[N].The New York Times（中文版）, 2013-07-02.

[482] ASHKAN SOLTANI B G.New documents show how the NSA infers relationships based on mobile location data[N].The Washington Post, 2013-12-10.

[483] BARTON GELLMAN A S.NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls[N].The Washington Post, 2014-03-18.

[484] AID M M.Inside the NSA’s ultra-secret China hacking group[M].The Foreign Policy 2013.

[485] BARTON GELLMAN E N.U.S.spy agencies mounted 231 offensive cyber-operations in 2011, documents show[N].The Washington Post, 2013-08-30.

[486] JACOB APPELBAUM L P, MARCEL ROSENBACH, CHRISTIAN STÖCKER, JÖRG SCHINDLER, HOLGER STARK.Inside TAO: documents reveal top NSA hacking unit[M].Der Spiegel, 2014.

[487] JENS GL SING L P, MARCEL ROSENBACH, HOLGER STARK.Fresh leak on US spying: NSA accessed Mexican President’s email[M].Der Spiegel, 2013.

[488] Photo gallery: NSA hacked into Mexican President’s email account[M].2013.

[489] Documents show N.S.A.efforts to spy on both enemies and allies[N].The New York Times, 2013-11-03.

[490] BAMFORD J.Sweat[M].Body of secrets: anatomy of the ultra-secret National Security Agency.Doubleday, 2001.

[491] ARTON GELLMAN A S.NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say[N].The Washington Post, 2013-10-30.

[492] LEOPOLD J.Emails reveal close Google relationship with

NSA[N].Aljazeera, 2014-05-06.

[493] What the ...?[M].Google Official Blog, 2013.

[494] 卢克·哈丁.斯诺登档案[M].北京：金城出版社，2014.

[495] 卢克·哈丁.斯诺登档案[M].北京：金城出版社，2014.

[496] GREENWALD G.THE FOURTH ESTATE[M].No place to hide: Edward Snowden, the NSA, and the US surveillance state.Metropolitan Books, 2014.

[497] 卢克·哈丁.斯诺登档案[M].北京：金城出版社，2014.

[498] HOPKINS N.UK gathering secret intelligence via covert NSA operation[N].The Guardian, 2013-06-07.

[499] HALLIDAY J.MoD serves news outlets with D notice over surveillance leaks[N].The Guardian, 2013-06-17.

[500] EWEN MACASKILL N D, NICK HOPKINS, JULIAN BORGER, JAMES BALL.GCHQ intercepted foreign politicians' communications at G20 summits[N].The Guardian, 2013-06-17.

[501] BORGER J.NSA files: why the Guardian in London destroyed hard drives of leaked files[N].The Guardian, 2013-08-20.

[502] 卢克·哈丁.斯诺登档案[M].北京：金城出版社，2014.

[503] EWEN MACASKILL G D.NSA Files: Decoded.2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[504] EDDY M.For western allies, a long history of swapping intelligence[N].The New York Times（中文版）, 2013-07-11.

[505] KHAZAN O.The creepy, long-standing practice of undersea cable tapping[M].The Atlantic.2013.

[506] CRAIG TIMBERG E N.Agreements with private companies

protect U.S.access to cables' data for surveillance[N].The Washington Post, 2013-07-06.

[507] CAMPBELL D.GCHQ's beyond top secret Middle Eastern internet spy base[M].The Register.2014.

[508] LAURA POITRAS M R, HOLGER STARK.Friendly Fire: How GCHQ monitors Germany, Israel and the EU[M].Der Spiegel, 2013.

[509] EWEN MACASKILL J B, NICK HOPKINS, NICK DAVIES, JAMES BALL.Analysis the legal loopholes that allow GCHQ to spy on the world[N].The Guardian, 2013-06-21.

[510] EWEN MACASKILL J B, NICK HOPKINS, NICK DAVIES, JAMES BALL.How does GCHQ's internet surveillance work?[N].The Guardian, 2013-06-21.

[511] DUNCAN CAMPBELL O W, JAMES CUSICK, KIM SENGUPTA.UK's secret Mid-East internet surveillance base is revealed in Edward Snowden leaks[N].The Independent, 2013-08-23.

[512] JAMES BALL L H, JULIETTE GARSIDE.BT and Vodafone among telecoms companies passing details to GCHQ[N].The Guardian, 2013-08-02.

[513] JOHN GOETZ H L, FREDERIK OBERMAIER, JAVIER C CERES.British officials have far-reaching access to internet and telephone communications[N].Süddeutsche Zeitung international, 2013-08-28.

[514] WHITE G.Spy cable revealed: how telecoms firm worked with GCHQ[J/OL].2014, http://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq.

[515] EWEN MACASKILL J B, NICK HOPKINS, NICK DAVIES, JAMES BALL.Mastering the internet: how GCHQ set out to spy on the world wide web[N].The Guardian, 2013-06-20.

[516] EWEN MACASKILL J B, NICK HOPKINS, NICK DAVIES,

JAMES BALL.GCHQ taps fibre-optic cables for secret access to world's communications[N].The Guardian, 2013-06-21.

[517] NICK HOPKINS J B, LUKE HARDING.GCHQ: inside the top secret world of Britain's biggest spy agency[N].The Guardian, 2013-08-02.

[518] SHUBBER K.A simple guide to GCHQ's internet surveillance programmeTempora[M].Wired, 2013.

[519] CHARLIE SAVAGE C C M, NICOLE PERLROTH.N.S.A.said to tap Google and Yahoo abroad[N].The New York Times, 2013-10-30.

[520] AUERBACH D.MUSCULAR 'Roid Rage![M].Slate, 2013.

[521] CRAIG TIMBERG B G, ASHKAN SOLTANI.Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic[N].The Washington Post, 2013-11-26.

[522] HEARN M.Googlers say "F*** you" to NSA, company encrypts internal network[J/OL].2013, http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/.

[523] STROHM C.Google's Schmidt sees encryption killing censorship[M].Bloomberg Business, 2013.

[524] MINERS Z.Yahoo turns on encryption between data centers[M].PCWorld, 2014.

[525] METZ C.Clash of the Titans! Inside Microsoft's battle to foil the NSA[M].The Wired.2013.

[526] ALAN RUSBRIDGER E M.I, spy: Edward Snowden in exile[N].The Guardian, 2014-07-19.

[527] NICK HOPKINS J B.NSA pays £100m in secret funding for GCHQ[N].The Guardian, 2013-08-01.

[528] BAMFORD J.Fat[M].Body of secrets: anatomy of the ultra-secret National Security Agency.Doubleday, 2001.

[529] ALDRICH R J.Schooldays[M].GCHQ: the Uncensored story of Britain's most secret intelligence agency.Harper Press, 2010.

[530] BAMFORD J.Memory[M].Body of secrets: anatomy of the ultra-secret National Security Agency.Doubleday, 2001.

[531] 阿萨–布里格斯.英国黑室："二战"中布莱奇利庄园的秘密岁月[M].北京：金城出版社，2014.

[532] ALDRICH R J.Friends and Allies[M].GCHQ: the Uncensored story of Britain's most secret intelligence agency.Harper Press, 2010.

[533] NORTON-TAYLOR R.Not so secret: deal at the heart of UK-US intelligence[N].The Guardian, 2010-06-25.

[534] GARDHAM D.Document that formalised 'special relationship' with the US[N].Telegraph, 2010-06-24.

[535] ALDRICH R J.UKUSA - Creating the Global SIGINT Alliance[M].GCHQ: the uncensored story of Britain's most secret intelligence agency.Harper Press.2010.

[536] COX J.Canada and the five eyes intelligence community[J/OL].2012, http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

[537] PERRONE J.The Echelon spy network[N].The Guardian, 2001-05-29.

[538] CAMPBELL D.Echelon: World under watch, an introduction[J/OL].2000, http://www.zdnet.com/echelon-world-under-watch-an-introduction-3002079845/.

[539] CAMPBELL D.Somebody's listening[J].New Statesman, 1988.

[540] BO ELKJAER K S.Echelon was my baby[N].EkstraBladet, 1999-11-17.

[541] ASSER M.Echelon: Big brother without a cause?[J/OL].2000, http://news.bbc.co.uk/2/hi/europe/820758.stm.

[542] Committee background documents on the U.S.Government advocacy center[M].2001.

[543] CAMPBELL D.Inside Echelon[J/OL].2000, http://www.heise.de/tp/artikel/6/6929/1.html.

[544] KOPSTEIN J.The NSA Can 'Collect-it-All,' But What Will It Do With Our Data Next?[J/OL].2014,http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html.

[545] HARRIS S.The Cowboy of the NSA[M].The Foreign Policy, 2013.

[546] ALDRICH R J.NSA and the ZIRCON Project[M].GCHQ: the uncensored story of Britain's most secret intelligence agency.Harper Press, 2010.

[547] ALDRICH R.Allied code-breakers co-operate – but not always[N].The Guardian, 2010-06-24.

[548] ALDRICH R J.Unmasking GCHQ: the ABC trial[M].GCHQ: the Uncensored Story of Britain's Most Secret Intelligence Agency Harper Press, 2010.

[549] SESEK R.Unraveling NSA's TURBULENCE Programs[M].2014.

[550] J.APPELBAUM A G, J.GOETZ, V.KABISCH, L.KAMPF, L.RYGE.NSA targets the privacy-conscious[J/OL].2014, http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html.

[551] LAURA POITRAS G G.Edward Snowden: 'The US

government will say I aided our enemies' – video interview[M].The Guardian, 2013.

[552] GREENWALD G.XKeyscore: NSA tool collects 'nearly everything a user does on the internet'[N].The Guardian, 2013-07-31.

[553] BALL J.Xbox Live among game services targeted by US and UK spy agencies[N].The Guardian, 2013-12-09.

[554] VOORHEES J.Bull Run, Manassas: why is the NSA naming its secret programs after battles we had with ourselves?[M].Slate, 2013.

[555] BAMBORD J.Brain[M].Body of secrets: anatomy of the ultra-secret National Security Agency.Doubleday, 2001.

[556] MCMILLAN R.The NSA is building a quantum computer? we already knew that[M].Wired, 2014.

[557] STEVEN RICH B G.NSA seeks to build quantum computer that could crack most types of encryption[N].The Washington Post, 2014-01-02.

[558] SCHNEIER B.What exactly are the NSA's 'groundbreaking cryptanalytic capabilities' ?[M].Wired, 2013.

[559] JAMES BALL J B, GLENN GREENWALD.How US and UK spy agencies defeat internet privacy and security[N].The Guardian, 2013-09-06.

[560] NICOLE PERLROTH J L, SCOTT SHANE.N.S.A.Able to foil basic safeguards of privacy on web[N].The New York Times, 2013-09-05.

[561] LEYDEN J.That earth-shattering NSA crypto-cracking: Have spooks smashed RC4?[M].The Register.2013.

[562] JACOB APPELBAUM A G, CHRISTIAN GROTHOFF, ANDY M LLER-MAGUHN, LAURA POITRAS, MICHAEL SONTHEIMER,

CHRISTIAN ST CKER.Prying eyes: inside the NSA's war on internet security[M].Der Spiegel, 2014.

[563] ZETTER K.Has the NSA been using the heartbleed bug as an internet peephole?[M].Wired, 2014.

[564] LEYDEN J.NSA spooks tooled up with zero-day PC security exploits from the FRENCH[M].The Register, 2013.

[565] JOYE C.Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander[M].The Australian Financial Review, 2014.

[566] ZETTER K.Obama: NSA must reveal bugs like heartbleed, unless they help the NSA[M].Wired, 2014.

[567] Michael Hayden[J/OL].2001, http://www.businessofgovernment.org/interview/michael-hayden-interview.

[568] Inside the NSA: the secret world of electronic spying[J/OL].2001, http://edition.cnn.com/TRANSCRIPTS/0103/25/sm.16.html.

[569] Statement for the record by Lieutenant General Michael V.hayden, USAF Director, National Security Agency/Chief, Central Security Service before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence[M].The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 2002.

[570] WILLIAM BINNEY A B."We had to wait for Snowden for proof ", an exchange with William Binney[J/OL].2014, https://www.opendemocracy.net/william-binney-anthony-barnett/%E2%80%9Cwe-had-to-wait-for-snowden-for-proof%E2%80%9D-exchange-with-william-binney.

[571] HARRIS S.Ships passing in the night[M].The Watchers: The

Rise of America's Surveillance State.Penguin Group, 2011.

[572] SHARKEY J B.Total Information Awareness[M].DARPATech 1999 Symposium.1999.

[573] HARRIS S.The Genoa project[M].The watchers: The rise of America's surveillance state.Penguin Group, 2011.

[574] JR.R O H.Total information awareness[M].No place to hide.Free Press.2006.

[575] ADAM MAYLE A K: The center for public integrity, 2002.

[576] MARKOFF J.Chief takes over at agency to thwart attacks on U.S.[N].The New York Times, 2002-02-13.

[577] MARKOFF J.Chief takes over new agency to thwart attacks on U.S.[N].The New York Times, 2002-02-13.

[578] HARRIS S.Call to arms[M].The Watchers: the rise of America's surveillance state.Penguin Group, 2011.

[579] HARRIS S.Full steam ahead[M].The watchers: the rise of America's surveillance state.Penguin Group, 2011.

[580] POINDEXTER J.OVERVIEW OF THE INFORMATION AWARENESS OFFICE[M].DARPATech 2002 Symposium, 2002.

[581] MARKOFF J.Poindexter's still a technocrat, still a Lightning Rod[N].The New York Times, 2003-01-20.

[582] 陈磊.钱学森的百年人生（上）[J/OL].2011, http://old.stdaily.com/special/content/ 2011-12/07/content_395868.htm.

[583] ARMOR T.Genoa II[M].DARPA Tech 2002 Symposium.2002.

[584] DYER D.Genisys[M].DARPA Tech 2002 Symposium.2002.

[585] TAIPALE K A.Data mining and domestic security:

connecting the dots to make sense of data[J].Columbia Science and Technology Law Review, 2003, 5(2).

[586] SENATOR T.Evidence extraction and link discovery program[M].DARPA Tech 2002 Symposium, 2002.

[587] WAYNE C.Human language technology TIDES, EARS, babylon[M].DARPA Tech 2002 Symposium, 2002.

[588] MARKOFF J.Pentagon plans a computer system that would peek at personal data of Americans[N].The New York Times, 2002-11-09.

[589] Poindexter opts for demotion, to stay in navy[N].Los Angeles Times, 1987-1987-03-07.

[590] JR.R O H.U.S.hopes to check computers globally: system would be used to hunt terrorists[N].The Washington Post, 2002-11-12.

[591] SAFIRE W.You are a suspect[N].The New York Times, 2002-11-14.

[592] SCARDAVILLE M, WebMemo 175[R]: The Heritage Foundation, 2002.

[593] SMITH M.Calling all Yahoos[M].SF Weekly, 2002.

[594] HARRIS S.The Unraveling[M].The watchers: the rise of America's surveillance state.Penguin Group, 2011.

[595] BENNETT A.Senators want to block government data mining[M].IT World, 2003.

[596] CLYMER A.THREATS AND RESPONSES: ELECTRONIC SURVEILLANCE; Congress agrees to bar Pentagon from terror watch of Americans[N].The New York Times, 2003-02-12.

[597](DARPA) DARPA, 2003.

[598] HARRIS S.Going black[M].The Watchers: The Rise of

America’s Surveillance State.Penguin Group, 2011.

[599] CLYMER A.New name of Pentagon data sweep focuses on terror[N].The New York Times, 2003-05-21.

[600] WEIGLE B D, AD-A 469632[R]: U.S.Amry war college, 2007.

[601] HANSON R.Policy Analysis Market: A Thwarted Experiment[J].Innovations, 2007, 2(3).

[602] HANSON R.The Policy Analysis Market (and FutureMAP) Archive.http://hanson.gmu.edu/policyanalysismarket.html.

[603] Pentagon threat-bet program to be canceled[N].USA Today, 2003-07-29.

[604] 美五角大楼放弃对未来恐怖事件下注“赌场计划”[J/OL].2003, http://www.chinanews.com/n/2003-07-30/26/329669.html.

[605] 陈威霖邓.认识“预测市场”——浅析这一预测工具及其于情报发现中的应用[J].情报杂志，2009，28(10).

[606] 李建标赵.预测市场机制的研究进展与展望[J].科学学与科学技术管理，2012, 33(8).

[607] STIGLITZ J E.Terrorism: there’s no futures in it[N].Los Angeles Times, 2003-07-31.

[608] Pentagon’s ‘terror information awareness’ program will end[N].USA Today, 2003-09-25.

[609] House Report 108-283[R].House of Representatives, 2003.

[610] HARRIS S.TIA Lives On[J].National Journal, 2006,

[611] GREENWALD G.Inside the mind of NSA chief Gen Keith Alexander[N].The Guardian, 2013-09-15.

[612] HEIL E.NSA director inherited Star Trek digs[N].The Washington Post, 2013-09-16.

[613] HARRIS S.Basketball[M].The watchers: the rise of America's surveillance state.Penguin Group, 2011.

[614] SNIFFEN M J.U.S.High-tech spy agency has low profile[N].The Washington Post, 2004-2-22.

[615] MARKOFF J.Experts say technology is widely disseminated inside and outside military[N].The New York Times, 2003-05-21.

[616] Novel Intelligence from Massive Data (NIMD).2002, http://web.archive.org/web/20030604181800/ic-arda.org/Novel_Intelligence/index.html.

[617] HARRIS S.Killer App[M].The Washingtonian, 2012.

[618] SCHEER R.The Military-Intelligence Complex[M].They know everything about you: how data-collecting corporations and snooping government agencies are destroying Democracy.Nation Books, 2015.

[619] BOWDEN M.The Targeting Engine[M].The finish: the killing of Osama Bin Laden.Atlantic Monthly Press, 2012.

[620] ANDY GREENBERG R M.How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut[M].Forbes, 2013.

[621] HALLECK T.Palantir technologies: the big data firm that purportedly helped kill Bin Laden just raised $50 Million[M].International Business Times, 2014.

[622] FEIN G.Director, national intelligence set to launch new intel research activity[N].C4I News, 2007-05-24.

[623] Latest M Square Tenant opens door to new research possibilities[M].Research@Maryland, 2008.

[624] KATHY LALLY J F.Bolivian president's plane forced to land in Austria in hunt for Snowden[N].The Washington Post, 2013-07-03.

[625] ANGELIKA GRUBER E F.Snowden still in Moscow despite Bolivian plane drama[J/OL].2013, http://www.reuters.com/article/2013/07/03/us-usa-security-snowden-idUSBRE9610C520130703.

[626] ROBERTS D.Bolivian president's jet rerouted amid suspicions Edward Snowden on board[N].The Guardian, 2013-07-03.

[627] MILLER G.U.S.officials scrambled to nab Snowden, hoping he would take a wrong step.He didn't.[N].The Washington Post, 2014-06-14.

[628] WILLIAM NEUMAN A S.Barring of Bolivian plane infuriates Latin America as Snowden case widens[N].The New York Times（中文版）, 2013-07-04.

[629] SPENCER ACKERMAN A H.NSA director Keith Alexander to speak at hacker conference in Las Vegas[N].The Guardian, 2013-07-11.

[630] ELLEN NAKASHIMA J W.For NSA chief, terrorist threat drives passion to 'collect it all'[N].The Washington Post, 2013-07-14.

[631] KAPLAN D.Black Hat: Alexander defends surveillance programs in keynote[M].SC Magazine, 2013.

[632] NAKASHIMA E.White House to preserve controversial policy on NSA, Cyber Command leadership[N].The Washington Post, 2013-12-13.

[633] PILKINGTON E.Guardian and Washington Post win Pulitzer prize for NSA revelations[N].The Guardian, 2014-04-14.

[634] STAFF G.Edward Snowden on Pulitzer winners: 'Their work has given us a better future'[N].The Guardian, 2014-04-14.

[635] DEANS J.Janine Gibson appointed editor-in-chief of theguardian.com[N].The Guardian, 2014-03-07.

[636] AULETTA K.Why Jill Abramson was fired[M].The New Yorker, 2014.

[637] SAVAGE C.Watchdog report says N.S.A.Program Is illegal and should end[N].The New York Times, 2014-01-23.

[638] ACKERMAN S.Some NSA data collection is 'legal and effective', says independent board[N].The Guardian, 2014-07-02.

[639] PINCUS W.Oversight board says NSA data mining puts citizens' privacy at risk but sees no abuse[N].The Washington Post, 2014-07-14.

[640] TSUKAYAMA H.New NSA chief says damage from Snowden leaks can be contained[N].The Washington Post, 2014-06-30.

[641] MCDUFFEE A.The NSA's moonlighting problem[M].The Atlantic, 2014.

[642] WARREN STROBEL M H.Ex-spy chief's private firm ends deal with U.S.official[J/OL].2014, http://www.reuters.com/article/2014/10/21/us-usa-intelligence-nsa-idUSKCN0IA2HV20141021.

[643] NAKASHIMA E.Obama signs off on nomination of Rogers as NSA director[N].The Washington Post, 2014-01-25.

[644] ACKERMAN S.NSA chief Michael Rogers: Edward Snowden 'probably not' a foreign spy[N].The Guardian, 2014-06-03.

[645] ELLEN NAKASHIMA E O K.Senate fails to advance legislation on NSA reform[N].The Washington Post, 2014-11-18.

[646] BIRNBAUM M.Russia grants Edward Snowden residency for three more years[N].The Washington Post, 2014-08-07.

[647] DAVIDSON A.Why “Citizenfour” Deserved Its Oscar[M].The New Yorker, 2015.

[648] MACASKILL E.Second leaker in US intelligence, says Glenn Greenwald[N].The Guardian, 2014-10-11.

后记

写作本书最初的念头来自于我偶然之间的阅读兴趣，希望做一点读书笔记来弥补不太够用的记忆力。没想到却像小学时读过的一本书里钓鱼的情景，一条鱼咬着前一条鱼的尾巴，有意思的东西越来越多。又有点儿像啃骨头，一寸一寸地，虽然困难但很有趣。参考资料越来越多，引用的资料也越来越多，我甚至不得不使用了专门的参考文献管理软件。我也知道写书很难，特别是想到自己的工作繁忙，身不由己的时候很多，所以起初并没有太大的雄心壮志。

接下来，有关的材料、线索多到让人透不过气来，有时兴奋，但更多的时候带有一些焦虑——苦苦寻觅不得其味、反复思索不得其解。很长一段时间，我每天只能睡着四五个小时，兴奋之中夹杂着焦虑，既快乐又苦闷。我知道，这样的日子要到把这本书完成才能结束。

书能写完，首先要感谢周倩博士。她是本书最初写好的两回的第一个读者。是她从那些粗糙的文字里发现了闪光之处，并且推荐给了中信出版社。我也因此结识了中信出版社的编辑。在计划完稿日期的促动下，我更加努力地进行写作。

王新女士是完整阅读本书初稿的第一个读者，她给我反馈了许多宝贵意见，帮助我克服掉一些自己难以察觉的写作陋习。翟玉成博士凭借他犀利的目光和渊博的知识，让原先在初稿中不时出现、搅乱故事的“我”彻底暴露并完全消除。孙宇军先生以及其他几位不愿署名的专家慷慨地和我分享了他们的经验和知识。王延飞教授、李法勇先生、童欣博士、秦利先生和靳天喜先生火一般的热情，激励我树立起坚定的信心。与李德顺博士的热烈讨论，使我身心愉悦，乐此不疲。高丽女士和王海波先生先后为我收集了多份有价值的资料，使得本书的叙述更为扎实可信。王馨博士在本书收尾之时，亲自帮我修改书稿，一番长谈，给了我新的启发和感受。

我还要感谢臧明先生和马雅莎女士，他们对于人生的深刻领悟和对于创作的独到见解，也促使我沉静心灵、反思自己。

方兴东先生和乔良教授在繁忙的工作之余抽出时间阅读了初稿，并

且写出褒扬有加的推荐序言，高度肯定了本书的价值，为这本书增添了光彩。

中信出版社为本书赋予了一个非常响亮的书名。出版社的编辑们运用扎实的文字功底打磨书稿，耐心细致地逐个核对繁多的参考文献，不厌其烦地回答我各种稀奇古怪的问题，为本书的最终完成提供了莫大的帮助。

最后，我还要感谢我的家人。年近古稀的父亲仔细阅读了初稿，发现了多处错误。母亲和即将初中毕业的孩子不时询问这本图书的进展，他们希望其能早日出版的心情溢于言表。夫人总是默默陪伴着我，她现在就坐在我的身后，看着我把这些文字打在屏幕上。

上述这些，是我完成本书的动力源泉。

于白居不易书房

2015年7月10日